# *i*STAR™ UU100 使用手冊

Release 2.3

**UUDynamics, Inc.**

**2004 年 12 月**

# 本書約定

## 描述：

文檔中對軟體中不同類型的元素，使用不同的符號和樣式進行描述（請參見下表）。請讀者使用本手冊之前務必認真閱讀，以便區分。

| 元素 | 符號＆樣式 | 字型大小 | 舉例 | 備註 |
| --- | --- | --- | --- | --- |
| 按鈕 | < > | 五號 | <確定> | |
| 功能表、快顯功能表 | “” | 五號 | “文件” | |
| 超鏈結 | 帶下劃線字體 | 五號 | 下一步 | |
| 參數 | [] | 小五號 | https://[*uuswitch 的IP 位址*](或[*uuswitch 的DNS 名稱*]) | |
| 螢幕回顯 | 斜體 | 小五號 | *ErrorCode[11001]:認證失敗* | []符號外部的內容，爲出錯提示，供使用者參考。[]內部的內容，爲系統內部資訊，供開放人員跟蹤。使用者可以不予理會，如有需要，亦可將其告知我公司技術支援人員。 |
| 重要、説明 | 加粗 | 五號 | **重要、** **説明** | |

## 解析度：

運行本產品，建議使用 800x600 或 1024x768 解析度，以獲得最佳視覺效果。

# 目 錄

# 第1章 概述

感謝您使用 UUDynamics 公司 ***i*STAR™**系列產品。***i*STAR™** UU100 是 UUDynamics 公司的一種伺服器版本發佈單元（Publisher）。

本使用手冊將對 ***i*STAR™**產品的功能特性及系統架構進行簡要描述，并在後面章節詳細介紹 UU100 的安裝、設定與操作步驟。

## 1.1 *i*STAR™產品功能特性

***i*STAR™**（**I**nstant **S**ecure **T**unnel **Ar**chitecture）是 UUDynamics 公司首創的新一代安全 Instant Extranet 技術。

***i*STAR™**用於構建由“發佈單元(Publisher)”向“用戶端(Subscriber)”發佈應用程式的 Extranet，這種方式能快速且安全地解決特定應用程式跨越企業網路和組織邊界的問題。***i*STAR™**技術提供了基于“用戶端（Subscriber）”、“發佈單元（Publisher）”和“交換單元(UUSwitch/UUExchange) ”的安全資訊網路模型，爲現代企業用戶和應用服務提供商（ASP）提供了應用程式或文件存取的發布、控制和管理平臺。同時，它涵蓋了傳統 VPN 的所有功能，爲現代企業網的 Intranet、Extranet、Remote Access、Application Export 等提供了安全、高效的整體解決方案；***i*STAR™**還能快速實現企業與其分支機搆和商業夥伴之間的 B2B、供應鏈、分散式 OA 等電子業務的需求。

與其他 VPN 產品相比，***i*STAR™**具有更強大的功能和更具優勢的性價比：

1. 安全性高：

   ***i*STAR™**采用了 SSL(Secure Socket Layer)協定，從應用層面建立安全機制，是 Application Sharing 的概念。通訊雙方在應用層建立通訊，除了能確保雙方的安全之外，也大幅降低規劃 IP 網路的複雜工程。

   - 采用了 SSL(Secure Socket Layer)協定。從應用層面建立安全機制，是 Application Sharing 的概念。通訊雙方在應用層建立通訊，實現應用層使用者訪問管理。徹底執行基於使用者的安全政策
   - 對應用程式透明。能夠保護企業網路免於遭受來自外部以及內部的威脅
   - 可以選擇對應用程式進行加密（Encryption & Hash）
   - 支援 Radius、Windows Domain 伺服器等多種使用者認證方式

2. 接入方式靈活：

   - 支援有公共靜態 IP 位址和沒有公共靜態 IP 位址的企業
   - 能爲企業夥伴提供安全的，彈性的外聯網(Extranet) 接入方式
   - 在任何時間，地點都能提供出外人員或遠端使用者即時，安全的接入
   - ***i*STAR™**獨特的對應用程式透明(Application Transparent)的特性，無論是 Web、client/server 應用程式，或是 file sharing，***i*STAR™**能够完全支援，不需要加裝軟體或對應用軟體作修改。支援 Web 、C/S 應用及 File Sharing
   - 支援 LAN To LAN 功能（僅 UU200 支援）

3. 提供路由功能：

UU200 和 UUSwitch/UUExchange 支援路由功能。

- 交換單元網路可以提供優化路由的選擇

- 具備爲遠端使用者提供優化路由的選擇

4. 經濟：

***i*STAR™**的另一項獨特設計就是能夠同時適應有 Public IP 及僅具備 Private IP 的使用環境，解決了部分企業 Public IP 資源不足帶來的問題，也避免了使用 Public IP 而引發的安全性問題。

由於可以使用 Private IP，因此企業的應用軟體伺服器能够被放置在內部網路的任何位置，而保護這些伺服器的網路與防火墻也不需要做任何改變，真正的作到了適應不同網路架構的需求。

- 可以共用數位電子憑證

  ***i*STAR™**還能夠將一張 SSL 數位電子憑證共用給多個使用 Private IP 的 Site 使用，節省了企業重複申請 SSL 數位電子憑證的費用。

- 充分利用互聯網以降低龐大的通訊成本

  采用了 SSL(Secure Socket Layer)協定。通訊雙方在應用層建立通訊，除了能確保雙方的安全之外，也大幅降低規劃 IP 網路的複雜工程。

- 控制網路建設、擴容、管理、使用及維護的整體成本（TCO: Total Cost of Ownership）

5. 使用者介面友好：

- 設備操作簡單，安裝容易
- 用戶端使用 IE 瀏覽器，各種應用都以圖示表示
- 提供多語言使用者介面支援

## 1.2 iSTAR™產品系統架構

***i*STAR™**的系統結構如下圖所示：

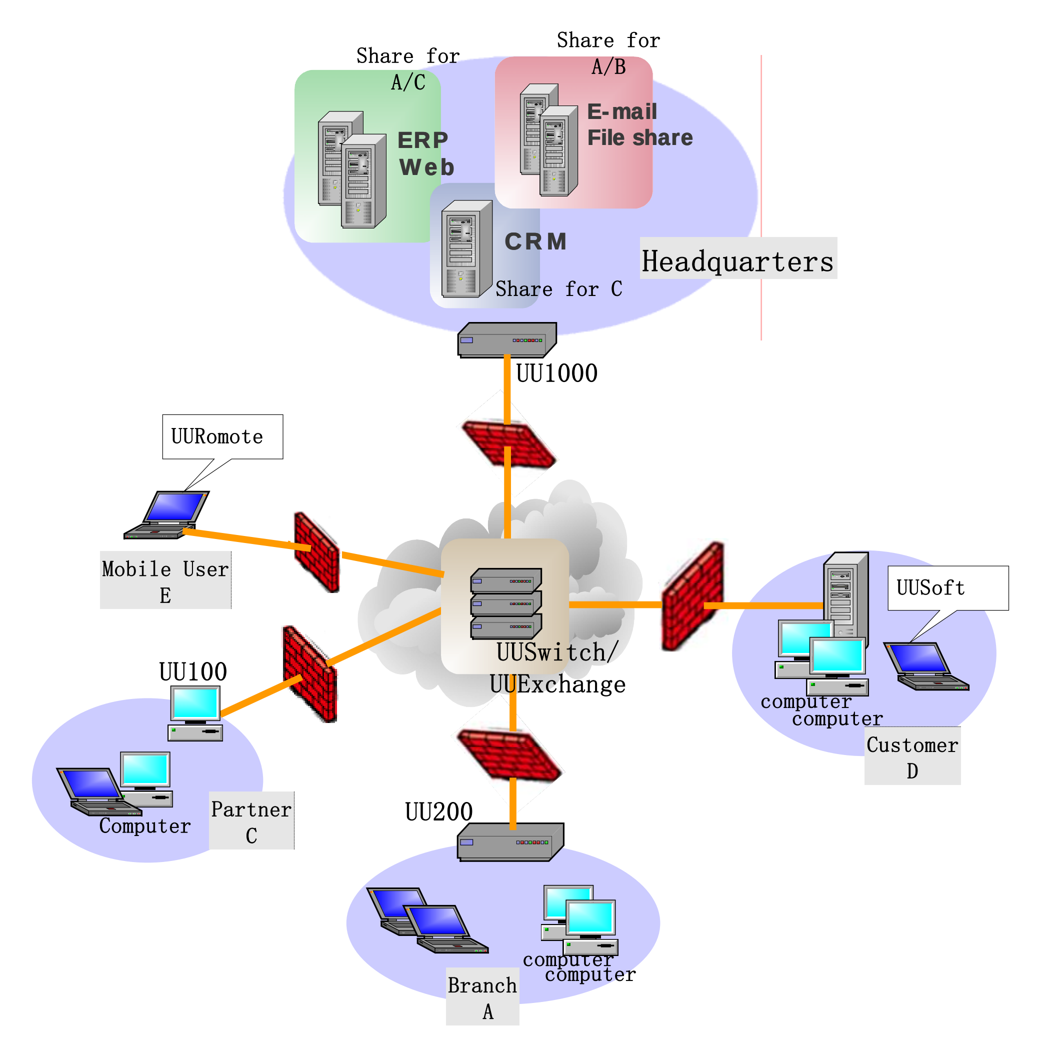



圖 1

如上圖所示，公司總部（headquarter）、合作夥伴(Partner)、分支機構(Branch)和移動客戶(Customer)間建立 ***iSTAR™*** 系統結構，分別以 UU200、UU100、UU1000 和中間的 UUSwitch/UUExchange 連接建立安全隧道；公司總部發布共用的應用給特定使用者，合作夥伴、分支機構等使用該些應用，從而實現了 Instant Extranet。UU1000/UU200/UU100 均具備發佈單元的功能；用戶端通過 IE/HTTPS 與伺服器相連接。***iSTAR™***技術中主要構成元件簡要介紹如下。

**交換單元(UUSwitch/UUExchange)**

UUSwitch/UUExchange 是 ***iSTAR™*** 系統結構的中心，它類似于電話系統中的交換中心，是高效的、均衡負載的伺服器群集或群集組，它負責維護著合法使用者資料庫，具有 Public Static IP 位址，在兩方進行應用資料交換之前提供“信令交換”的功能；UUSwitch/UUExchange 能物理上分佈在多個地點上，透明地轉發應用資料。

**發佈單元（Publisher）**

發佈單元（Publisher）UU100/UU200/UU1000 位於 ***iSTAR™***中發布應用的伺服器端，它可以將伺服器提供的服務安全的發布。

**用戶端（Subscriber）**

用戶端通過 IE/HTTPS 與伺服器相連接。

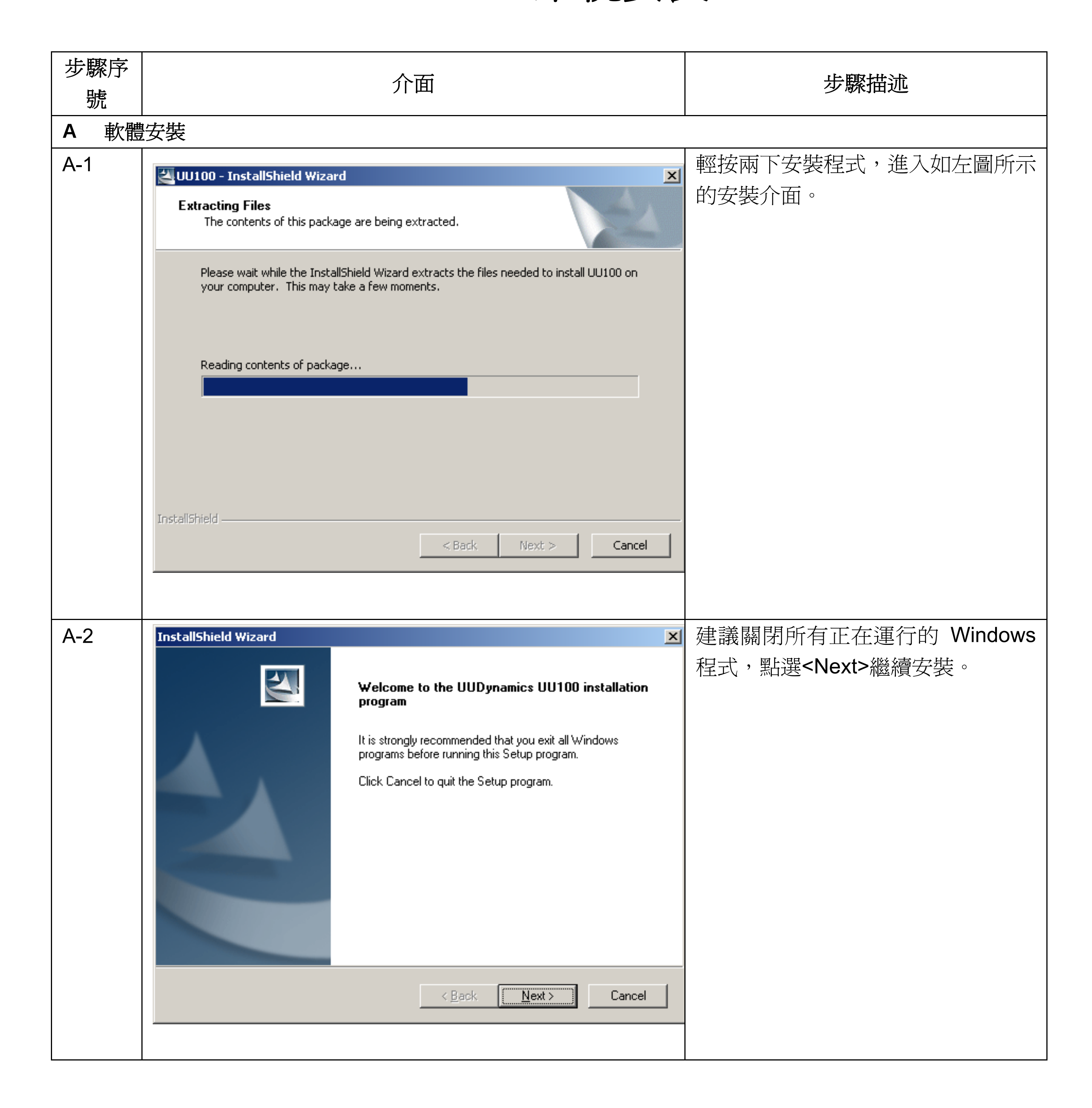
**Registration (Logical Naming)**

每個發佈單元 Publisher 都必須配置成能夠到達 UUExchange，並且都有一個唯一的邏輯名稱 UUID，在啓動時就用這個邏輯名稱註冊到 UUSwitch/UUExchange,從而成爲整個 ***i*STAR™**的一部分。所以發佈單元本身不一定需要 Public Static IP 位元元元址。

**End to End Security Connectivity**

資訊安全的含義主要包含以下幾個方面：用戶端和伺服器端的認證、資訊的私密性、資訊的完整性和授權。***i*STAR™**結構中的發布單元和用戶端之間的隧道是基于 SSL 的安全連接，同時滿足以上幾個方面，實現端到端的安全。

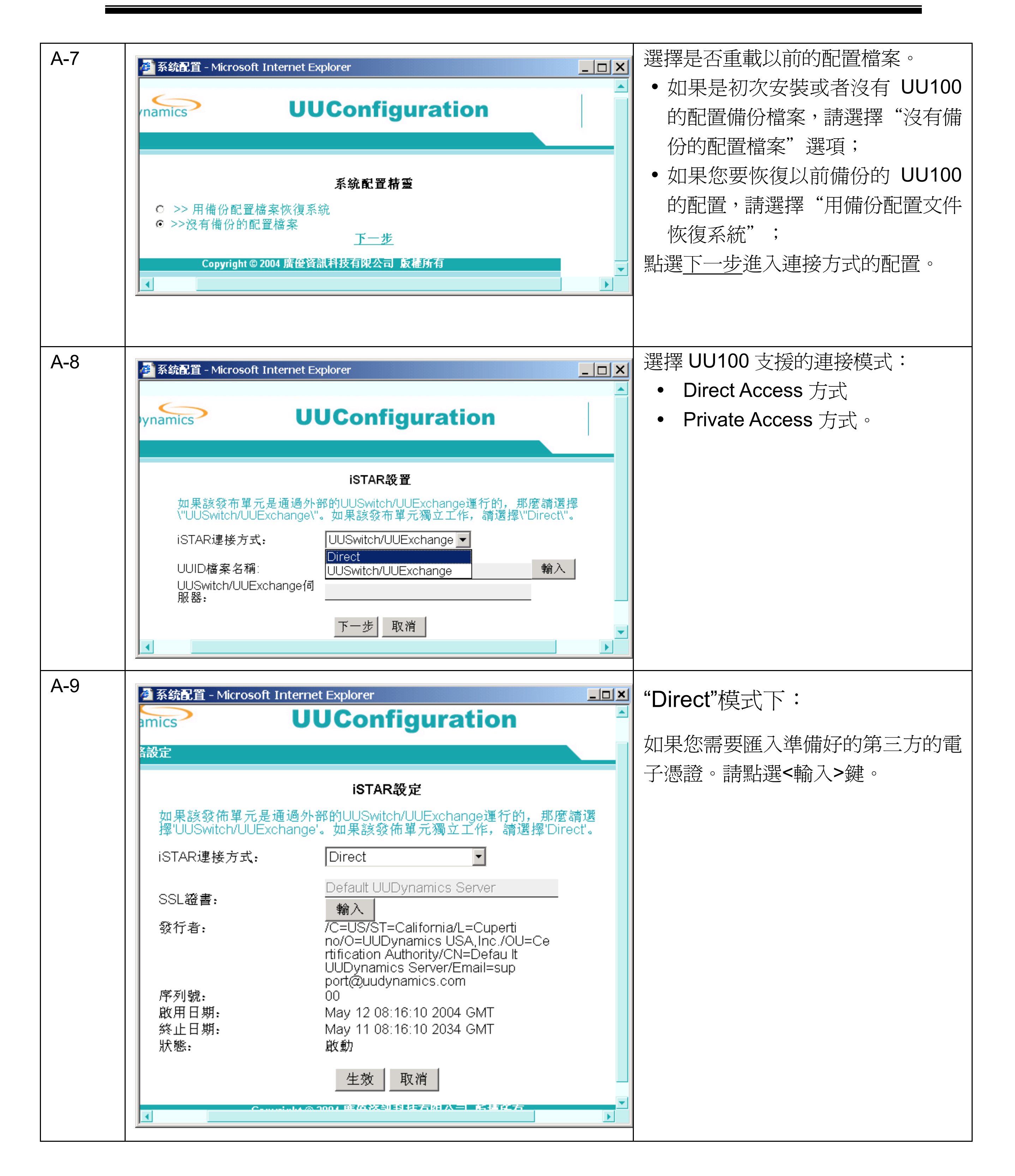
# 第2章　系統安裝




| 步驟序號 | 介面 | 步驟描述 |
| --- | --- | --- |
| **A** 軟體安裝 | | |
| A-1 | | 輕按兩下安裝程式，進入如左圖所示的安裝介面。 |
| A-2 | | 建議關閉所有正在運行的 Windows 程式，點選<Next>繼續安裝。 |



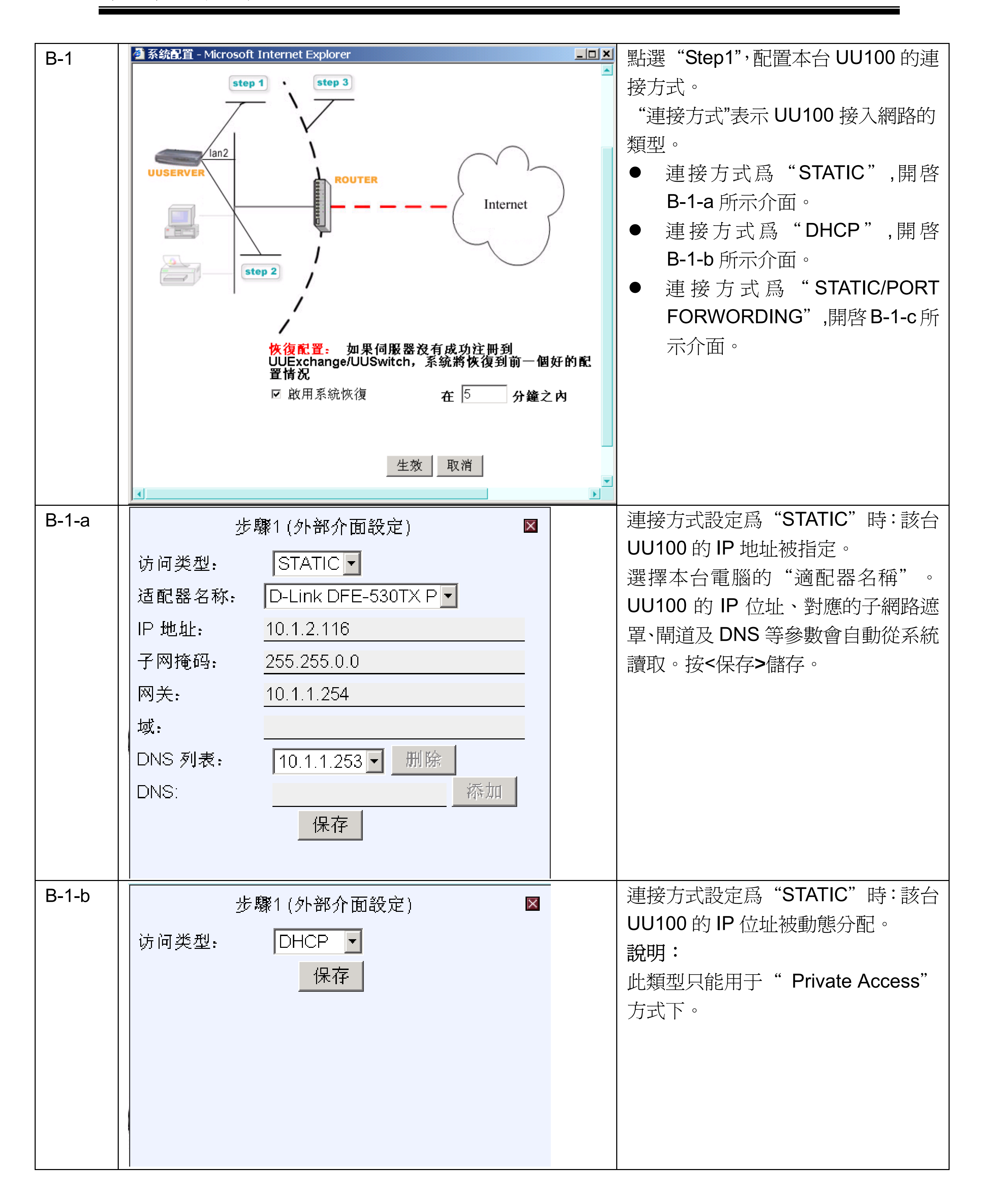

| 步驟 | 畫面 | 說明 |
|---|---|---|
| A-3 | | 安裝前，請先閱讀版權頁面。<br>如果同意所有內容，點選<Yes>繼續安裝。<br>否則，點選<No>退出安裝。 |
| A-4 | | 選擇安裝路徑。點選<Browser>可以改變安裝路徑。<br>點選<Next>繼續安裝。 |
| A-5 | | 輸入文件夾名稱，該名稱將顯示在 Windows 主介面【開始】程式列表中。<br>點選<Next>繼續安裝。 |
| A-6 | | 點選<確定>繼續安裝。 |



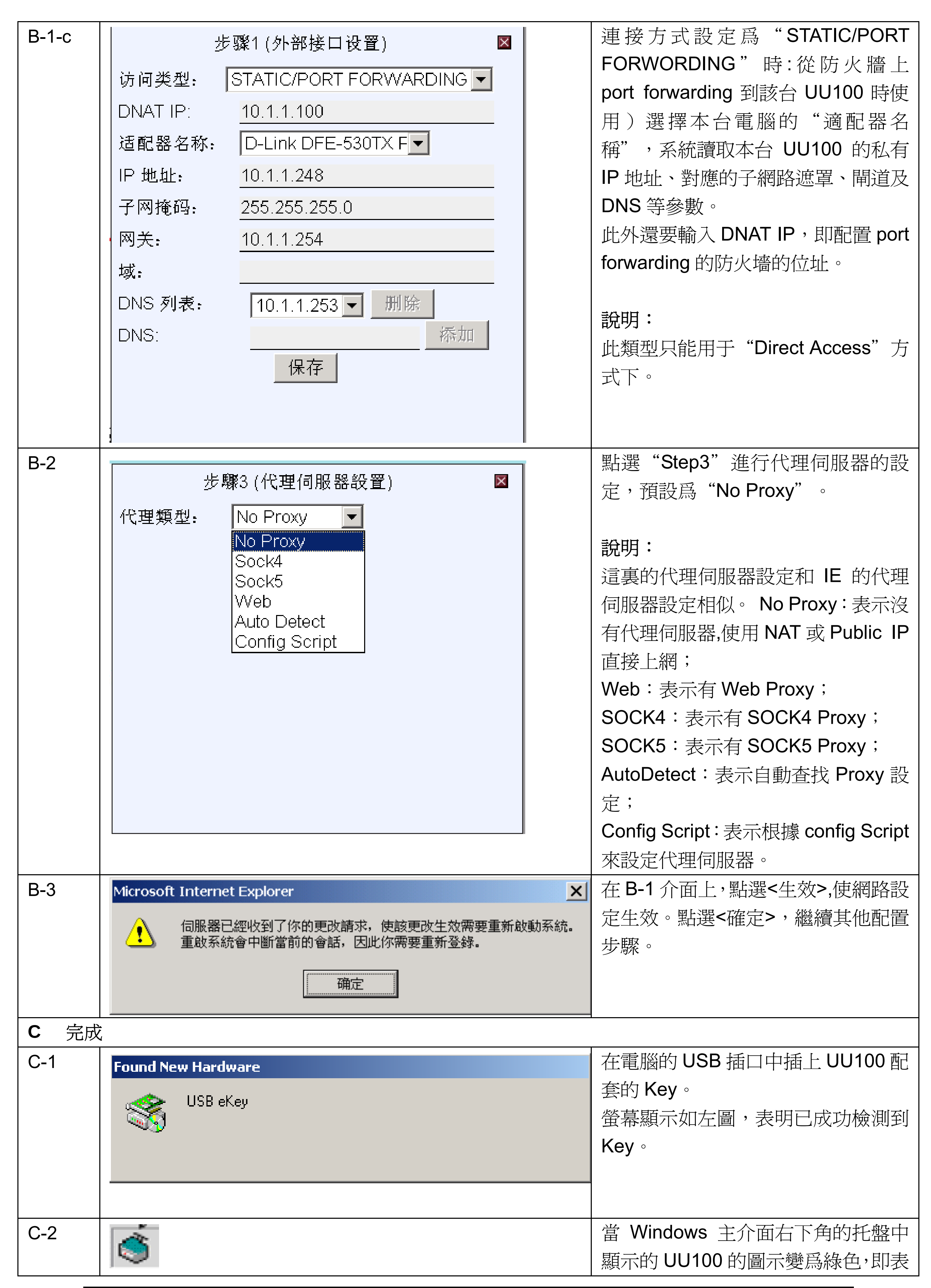
| 步驟 | 畫面 | 說明 |
|---|---|---|
| A-7 | 系統配置精靈：>> 用備份配置檔案恢復系統／>>沒有備份的配置檔案／下一步 | 選擇是否重載以前的配置檔案。<br>• 如果是初次安裝或者沒有 UU100 的配置備份檔案，請選擇“沒有備份的配置檔案”選項；<br>• 如果您要恢復以前備份的 UU100 的配置，請選擇“用備份配置文件恢復系統”；<br>點選下一步進入連接方式的配置。 |
| A-8 | iSTAR設置：iSTAR連接方式（Direct／UUSwitch/UUExchange） | 選擇 UU100 支援的連接模式：<br>• Direct Access 方式<br>• Private Access 方式。 |
| A-9 | iSTAR設定：iSTAR連接方式 Direct；SSL證書 | “Direct”模式下：<br>如果您需要匯入準備好的第三方的電子憑證。請點選<輸入>鍵。 |



| | | |
|---|---|---|
| A-9-a | | 輸入該證書對應的 Key 檔案，證書檔案和 CA 的證書檔案，所有檔案要求是 Base64 編碼方式。<br>點選<更新>，返回上層頁面。<br>說明：<br>第三方電子憑證的更多資訊請參見“術語表”。 |
| A-10 | | UUSwitch/UUExchange 模 式下：<br>點選<輸入>,導入 UUID 檔案。(見 A-10-a)<br>輸入 UUSwitch/UUExchange 的 IP 位址或 DNS 名稱。<br>最後按<生效>鍵，使當前的連接模式設定生效。 |
| A-10-a | | 點選<瀏覽>,導入 UUID 檔案，(這裏的 UUID 檔案由在這裏輸入的 UUSwitch/UUExchange 產生得到)。<br>如果該 UUID 文件有密碼保護，請先勾選“密碼”,並輸入密碼。<br>點選“更新”,確認幷返回上一介面。 |
| **B** 網路設定 | | |

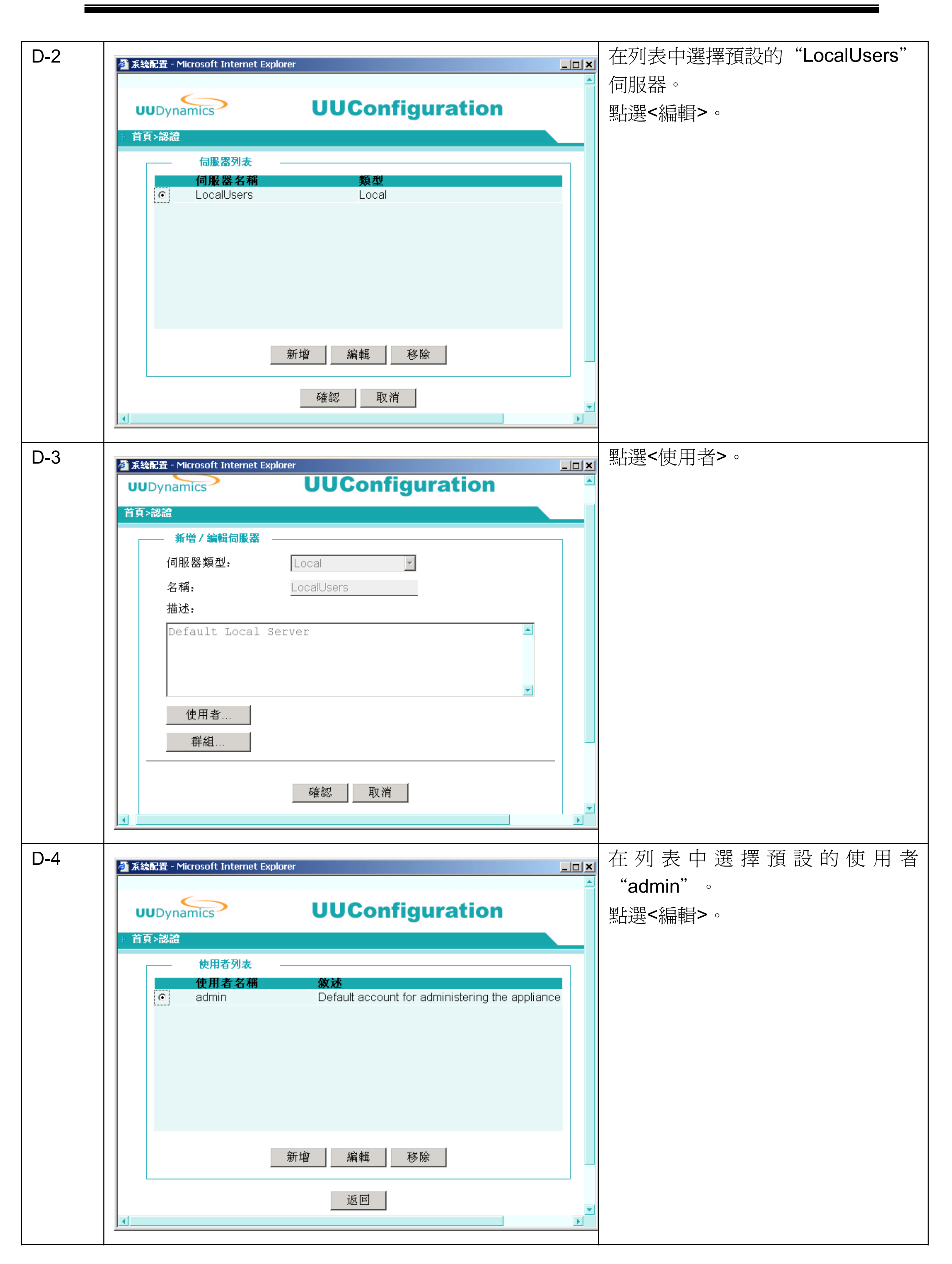



| | | |
|---|---|---|
| B-1 | | 點選 “Step1”，配置本台 UU100 的連接方式。<br>“連接方式”表示 UU100 接入網路的類型。<br>● 連接方式爲 “STATIC” ,開啓 B-1-a 所示介面。<br>● 連接方式爲 “DHCP” ,開啓 B-1-b 所示介面。<br>● 連接方式爲 “STATIC/PORT FORWORDING” ,開啓 B-1-c 所示介面。 |
| B-1-a | | 連接方式設定爲 “STATIC” 時：該台 UU100 的 IP 地址被指定。<br>選擇本台電腦的 “適配器名稱” 。UU100 的 IP 位址、對應的子網路遮罩、閘道及 DNS 等參數會自動從系統讀取。按<保存>儲存。 |
| B-1-b | | 連接方式設定爲 “STATIC” 時：該台 UU100 的 IP 位址被動態分配。<br>**說明：**<br>此類型只能用于 “ Private Access” 方式下。 |

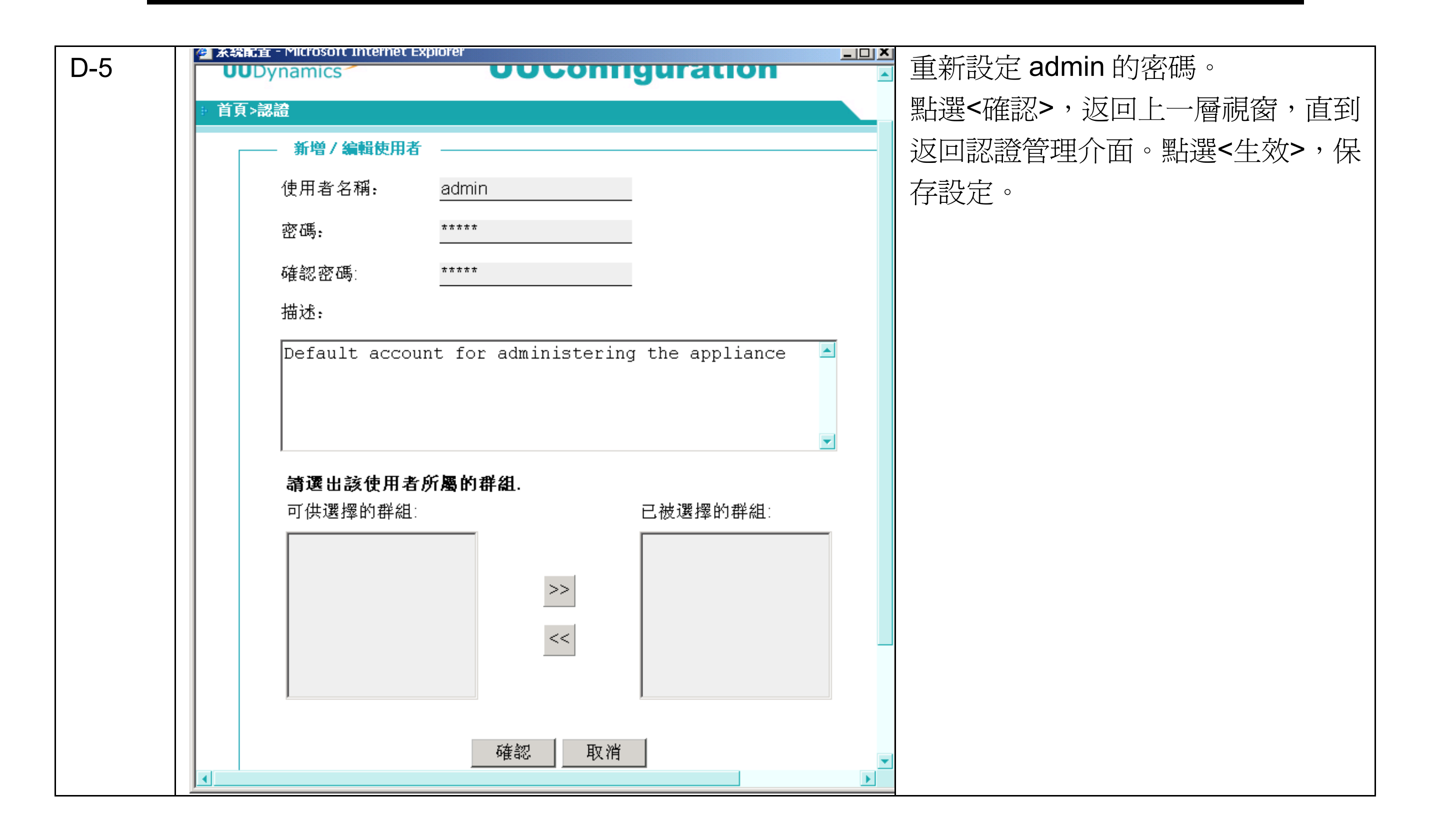



| 步驟 | 說明 |
|---|---|
| B-1-c | 連接方式設定爲 “STATIC/PORT FORWORDING” 時：從防火牆上 port forwarding 到該台 UU100 時使用）選擇本台電腦的 “適配器名稱”，系統讀取本台 UU100 的私有 IP 地址、對應的子網路遮罩、閘道及 DNS 等參數。<br>此外還要輸入 DNAT IP，即配置 port forwarding 的防火墻的位址。<br><br>**說明：**<br>此類型只能用于 “Direct Access” 方式下。 |
| B-2 | 點選 “Step3” 進行代理伺服器的設定，預設爲 “No Proxy” 。<br><br>**說明：**<br>這裏的代理伺服器設定和 IE 的代理伺服器設定相似。 No Proxy：表示沒有代理伺服器,使用 NAT 或 Public IP 直接上網；<br>Web：表示有 Web Proxy；<br>SOCK4：表示有 SOCK4 Proxy；<br>SOCK5：表示有 SOCK5 Proxy；<br>AutoDetect：表示自動查找 Proxy 設定；<br>Config Script：表示根據 config Script 來設定代理伺服器。 |
| B-3 | 在 B-1 介面上，點選<生效>,使網路設定生效。點選<確定>，繼續其他配置步驟。 |
| **C** 完成 | |
| C-1 | 在電腦的 USB 插口中插上 UU100 配套的 Key。<br>螢幕顯示如左圖，表明已成功檢測到 Key。 |
| C-2 | 當 Windows 主介面右下角的托盤中顯示的 UU100 的圖示變爲綠色，即表 |

| | | |
|---|---|---|
| | | 示該 UU100 以被成功安裝和配置。可以正常使用了。 |
| C-3 |  | 將滑鼠懸停在 UU100 的圖示上，點選滑鼠右鍵選擇“Configuration”。在開啓的登入介面輸入使用者名稱/密碼（預設爲 admin/admin），即可開啓左圖所示介面，進行修改設定、發布應用、管理系統等操作。 |
| **D 修改管理員密碼**<br>爲保護系統安全，請在安裝結束後，立即修改管理員密碼。 | | |
| D-1 | UUConfiguration<br>LocalAdmin LocalUsers Local No<br>新增 / 編輯伺服器...<br>新增 / 編輯角色...<br>新增 / 編輯根證書...<br>新增 編輯 移除<br>生效 取消 | 在 C-3 所示介面中，點選 認證管理，開啓左邊的設定介面。<br>點選<新增/編輯伺服器>。 |




| | | |
|---|---|---|
| D-2 | | 在列表中選擇預設的“LocalUsers”伺服器。<br>點選<編輯>。 |
| D-3 | | 點選<使用者>。 |
| D-4 | | 在列表中選擇預設的使用者“admin”。<br>點選<編輯>。 |

| D-5 |  | 重新設定 admin 的密碼。<br>點選<確認>，返回上一層視窗，直到返回認證管理介面。點選<生效>，保存設定。 |
|---|---|---|

# 第3章 系統設定

完成上述 UU100 的系統安裝和初次配置之後，您可以隨時進行 UU100 的系統設定。

## 3.1 啓動 UU100

將遊標移到 Windows 桌面右下角的 UU100 圖示，按滑鼠右鍵選擇“Start”，可以啓動 UU100。當圖示變爲綠色則表示 UU100 啓動成功。

完成了 UU100 軟體的安裝和初次配置之後，在伺服器 Windows 桌面的右下角會有一個 UU100 顯示圖示，該圖示的顏色表示了 UU100 的狀態（見圖 2）：

- 紅色表示 UU100 處於停止狀態
- 黃色表示 UU100 正處於被啓動（或被停止）之中
- 綠色表示 UU100 已經啓動，處於運行正常狀態








圖 2

## 3.2 熟悉介面操作

### 3.2.1 進入設定介面

配置介面采用 WEB 方式，進入配置介面前需要登入。

可以通過本地和遠端兩種方式進入設定介面：

1. 在裝有 UU100 的機器上，將遊標移到伺服器 Windows 桌面右下角的 UU100 圖示，按下滑鼠右鍵，選擇“Configuration”功能表，輸入預設的使用者名稱和密碼(admin/admin)後，將會出現如圖 4 所示的系統主介面。
2. 遠端系統管理員可以在任何一台聯機到網際網路的電腦上通過 rm 方式開啓遠端使用者應用列表介面，即：在瀏覽器地址欄輸入“https://[*uuswitch* 或 *uuexchange 的 DNS 名稱/IP 位址*]/[*uu100 名稱*]/rm”（Private Access 方式）或“https://[*uu100 的 IP 位址*]/rm”(Direct Access 方式)，輸入使用者名稱、密碼。開啓遠端使用者應用列表介面。在該介面中輕按兩下“Admin”圖示，并在彈出的視窗中輸入預設的使用者名稱和密碼(admin/admin)後，也將出現如圖 4 所示的系統主介面。

如果使用者超過 10 分鐘後需要對系統繼續進行操作，系統會彈出圖 3 提示資訊，要求使用者重新登入。




圖 3

原因是系統處于安全考慮，設定了“Session Timeout”（會話超時）。Timeout 的時間爲 10 分鐘。

**重要：**

爲了保障系統及內部資料安全，UU100 安裝完成後，請務必修改 Admin 的密碼。修改 Admin 和其他使用者密碼的方法有以下兩種：

- 在圖 4 所示的系統主介面中，點選“安全管理”下的認證控制。選中某一使用者，點選<編輯>，即可在開啓的介面中修改該使用者的密碼。
- 通過 IE 瀏覽器，遠端系統管理員可以在任何一台聯機到網際網路的電腦上通過 rm 方式開啓遠端使用者應用列表介面，在開啓的介面中雙擊“更改密碼”圖示，即可在開啓的介面中修改該使用者的密碼。

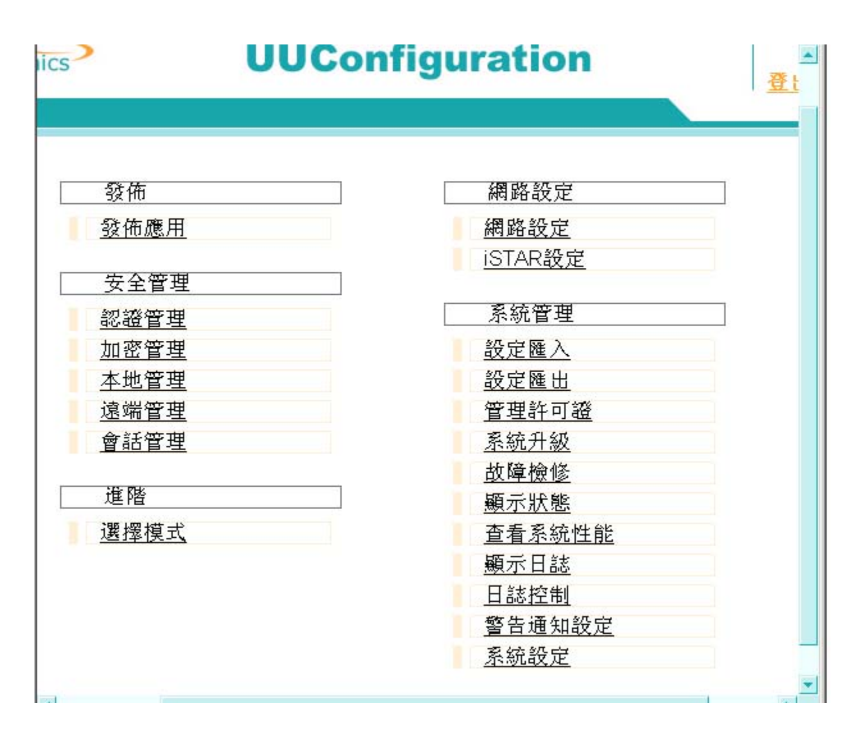



圖 4

介面中各配置項功能介紹如下。具體說明及操作步驟將在下文相應章節中詳細描述：

**【發布】**

發布應用：設定 Publisher 要發佈的應用，包括增加、刪除和編輯相關應用的功能，對於每個應用可以設定授權使用者和指定限制該應用訪問的地址和埠。

具體配置步驟請參見“第 4 章發佈應用”。

【安全管理】

認證管理：設定系統的認證類型，并根據系統的認證類型，進行相關配置。

加密管理：可以用于選擇資料安全傳輸的加密演算法和 Hash 演算法。

本地管理：對本地管理進行授權，授權使用者可以對系統進行本地管理。

遠端管理：對遠端管理進行授權，授權使用者可以對系統進行遠端管理。

會話管理：對連入的會話進行管理。

【進階】

選擇模式：模式選擇，包括單模式、透明模式和路由模式。根據系統在實際網路中的位置選擇具體的模式。

【網路設置】

網路設置：該模組用以設定系統所在的內部網路和 UUExchange/UUSwitch 的相關資訊（包括 IP 位址、子網路遮罩、閘道、代理伺服器、Internet 的接入方式等）。

iSTAR 設置：改變當前的連接方式。

【系統管理】

設定匯入：將原來保存好的配置文件導入到系統中。

設定匯出：將系統中已配置的配置文件導出到指定的文件夾保存。

管理許可證：輸入新的 License 檔案，更新當前 License。

升版系統：導入升版文件，升版當前的版本。

鼓掌檢修：選擇 Ping、TraceRoute、Netstat 命令檢測系統的網路運行狀況。

顯示狀態：查看系統的狀况，包括 UUServer 的類型、系統的模式、系統的當前運行狀態等，以及當前系統的模式等。

查看系統性能：查看系統的各種的統計資訊。

顯示日志：查看日誌。包括查看系統每天指定時間段中，由重點到詳細的日志情況，并可隨時保存日志，以便隨時審閱。

日志控制：系統日志的設定。

警告設定：系統報警級別的設定。

系統管理：系統伺服器的時間設定和 LOGO 的設定。

### 3.2.2 介面間的轉換

IE 瀏覽器上自帶的“Forward（前進）”、“Back(後退)”等按鈕及“文件”、“編輯”等功能表均不再出現在介面上。

- 返回上一級介面，請點選<返回>或<取消>鍵。
- 保存配置的修改，請點選<確認>或<保存>鍵。

### 3.2.3 退出設定介面

退出配置介面前，請退回到圖 4 所示配置介面，點選 登出 退出。否則，再次（或用同樣的使用者名稱從其他機器）登入時，系統將提示以下資訊 ：

*“User username logined on this system currently”*

此時，相同使用者或者管理權限更高的使用者可以勾選“中斷使用者[*username*]”，重新登入系統。

例如：使用者在上一次非正常退出後，可以勾選該選項，强制停止自己的帳號，重新登入系統。或者，管理員可以停止其他只有“唯讀”許可權的使用者帳號，但不能停止其他管理員帳號（詳細內容請參考“設定本地/遠端管理員”章節）。

📖 說明：

如果勾選“中斷使用者[*username*]”時出錯（如圖 5），有可能是因爲您沒有許可權使該使用者失效。如果仍要登入，請聯繫系統管理員。




圖 5

## 3.2.4 使設定生效

“生效”表示使您的配置生效。

修改配置後，點選<確認>或<保存>鍵進行保存，但此時僅是臨時性保存。一旦點選<取消>這些配置資訊有可能丟失。因此保存成功後，還必須點選<生效>，配置方可永久保存幷生效（圖 6）。

ⓘ 重要：

- 以下七項設定完成後，點選<生效>會中斷會話，同時系統會提示使用者重新登入。因此，建議您：避免在系統繁忙時改變這幾項設定。
  網路設置；iSTAR 設置；認證控制；設定匯入；
  選擇模式；管理許可證；升版系統；
- 點選<生效>後有時會重新啓動系統的服務，這時介面上可能會出現“非法 IP”等資訊，這時需要稍等片刻，重新進入配置介面。

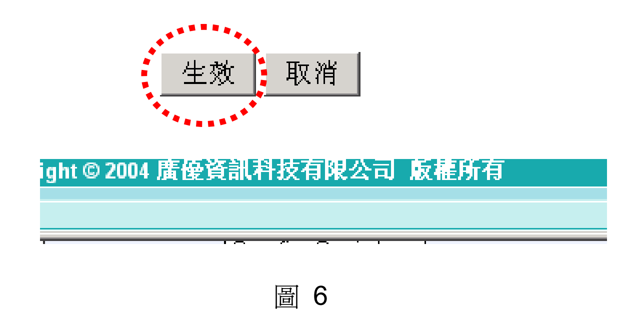


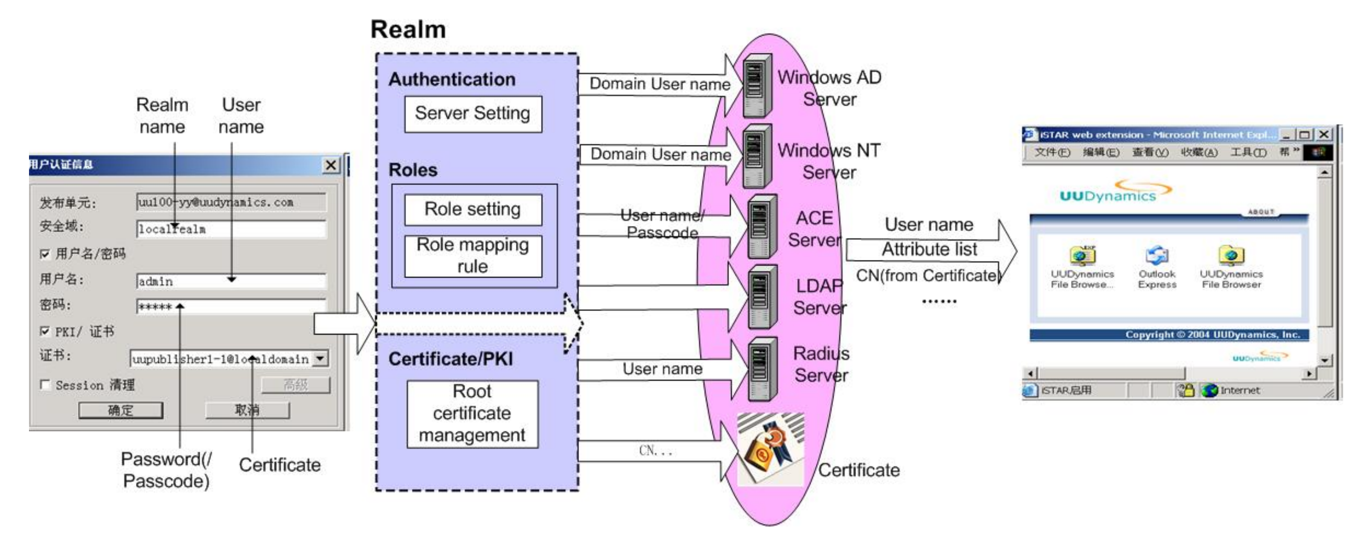

圖 6

## 3.3 用戶管理

UU200 的用戶包括管理員和使用者。管理者可以在本地或遠端對 UUSWITCH(/UUEXCHANGE)進行設定和維護，包括管理使用者帳號，升版系統、發布應用等。

### 相關概念：

UU200 用戶包括 UU200 管理員和遠端使用者。管理者可以在本地或遠端對 UU200 進行設定和維護，包括管理使用者帳號，升版系統、發布應用等。




UU200 允許管理員使用嚴密的安全控制方式，層層驗證接入安全。包括登入身份驗證、授權和應用級驗證策略等，杜絕了各種未經認證和授權的非法連接。

爲了實現這種安全控制思想，伺服器端（UU200）需要完成相關的設定。以下對涉及到的各種概念進行說明和舉例。

- 認證:身份驗證。認證伺服器用於驗證使用者端傳來的使用者名稱、證書等代表身份的資訊。身份驗證有以下幾種途徑：

1. 使用者端輸入的使用者名稱/密碼。如果使用者名稱和密碼不符，則驗證失敗。
2. 使用者端導入的證書的 CN 等屬性驗證。證書的可信任性由簽發的根證書負責。
3. 認證伺服器上該使用者相應的屬性。使用者屬性需要根據使用者名稱在指定的認證伺服器檢索和匹配。
4. 一次性有效的密碼。例如 RSA 的 token code。這種一次性有效的密碼通常用於雙因數身份認證。這種方式的認證要求使用者輸入使用者名稱、passcode（PIN

＋Token code）。

- 授權：應用授權。發布應用時通常將應用授權給已通過身份驗證的使用者。授權依據通常是以下一種或多種資訊：

1. 代表使用者身份的使用者名稱
2. 使用者隸屬的群組列表
3. 使用者對應的角色（從證書中的屬性以及使用者在認證伺服器上對應的屬性對應而來）。

- 規定：安全管理綜合策略。管理員可以根據安全級別組合各種包括身份驗證、授權在內的所有的安全管理方法。

  例如，當安全需求極高時，可以設定一種較嚴密的規定：使用雙因數身份認證（使用者名稱 + 證書）和通過另一張證書授權，即：Client 端必須同時提供使用者名稱和證書，并通過驗證另一張證書是否給該使用者授權或授權該使用者使用何種應用。

- Certificate/PKI（根證書）：證書。由 CA 簽發，包含使用者 CN 或其他屬性等安全資訊。

  通常用於驗證使用者的身份或對通過身份驗證的使用者進行應用授權。

- 角色:角色定義。

  PKI 和 Radius 類型的伺服器中，通常將一組相同屬性定義爲一個角色。使用者屬於某一角色意味著他（/她）具有相應的所有屬性。UU200 在 PKI 和 Radius 兩種類型的安全域中引入了角色這一概念，目的是方便將某一應用授權給某一角色（即具有某些相同屬性的使用者）。

  角色通常在驗證 AD/Radius 伺服器上的使用者身份和應用授權時作爲主要依據。

- 安全域：每一個使用者隸屬於一個或多個安全域。安全域代表了使用 iSTAR 產品時使用者的安全特徵。iSTAR 產品將依據域中的各項特徵逐一驗證使用者身份。

  在安全域中設定的內容包括：驗證使用者身份的伺服器、證書以及驗證策略等資訊。使用者隸屬于某個安全域，意味著該使用者將使用該域中指定的綜合安全管理策略，包括：在指定的認證伺服器或（/和）證書進行身份驗證，驗證通過後，UU200 將根據指定的授權策略或（/和）證書對使用者進行應用授權。安全域的使用可以參考以下例子。

  **說明：**

  本系統中有一個預設的安全域：LocalUsers。LocalUsers 中設定了一個預設的伺服器— LocalUsers，該伺服器中有預設的 User/密碼：admin/admin。預設的使用者 admin、伺服器和安全域不能被刪除。這樣可以保證至少有一位具有“唯讀/更改”許可權的使用者存在。

  LocalUsers 中不允許設定 Certificate/PKI。

## 實例：

例一：

- 背景

某企業爲大型銀行。使用者類型包括：區域網路路使用者、Radius、遠端存取使用者……

其中：

User1：本地使用者，安全需求一般。在 LocalSever 中驗證使用者名稱身份。企業的合作夥伴或代理商適合使用這種使用者身份連入企業的內部網。

User2：本地使用者，沒有使用者名稱/密碼，但持有某 CA 簽發的證書。

User3：Radius 使用者。安全需求高，在 Radius 伺服器上有使用者名稱/密碼，屬於某一角色。

User4：遠端使用者，安全需求極高，需要使用使用者名稱/Passcode(PIN+ Token code). 在 ACE 伺服器上驗證身份進行雙重身份認證。

Group1：成員包括 User1。

- 身份驗證設定

1. 預置以下幾個伺服器。

RadiusUsers：類型爲 Radius；

ACEUsers：類型爲 ACE/Server；

2. 預置以下幾個安全域。

LocalUsers：預設。不需增刪也不能更改。

PKIRealm: 新增。僅需要驗證證書。

| 設定項 | 值 | 說明 |
| --- | --- | --- |
| 使用以下伺服器進行認證/制定策略 | None | 類型：無 |
| 通過 Certificate/PKI 認證 | True | 選中該選項，並點選<管理證書>選擇信任的根證書。 |

RadiusRealm：新增。用於驗證 Radius 域的使用者。選擇 MyRadius 作爲認證伺服器。

| 設定項 | 值 | 說明 |
| --- | --- | --- |
| 使用以下伺服器進行認證/制定策略 | RadiusUsers | 類型：Radius |
| 通過 Certificate/PKI 認證 | False | 不選中該選項。 |
| 角色 | | 點選<增加/編輯映射規定…>，可以增加/編輯角色的對應規定。 |

ACERealm：新增。用於驗證遠端使用者。

| 設定項 | 值 | 說明 |
| --- | --- | --- |
| 使用以下伺服器進行認證/制定策略 | ACEUsers | 類型：ACE |
| 通過 Certificate/PKI 認證 | False | 不選中該選項。 |

3. 將使用者/群組按安全需求加入到相應的安全域中。

User1/Group1：加入 LocalUsers。使用使用者名稱/密碼在 Local 伺服器上認證身份。

User2：加入 PKIRealm，沒有使用者名稱/密碼，但持有某 CA 簽發的證書。通過證書中 CN 或其他屬性驗證使用者身份。驗證通過後，從證書中獲取該使用者的屬性，進行應用授權。

User3：加入 RadiusRealm，在 Radius 伺服器上驗證使用者名稱/密碼，驗證通過後，從 Radius 伺服器上獲取該使用者的屬性，進行應用授權。

User4：加入 ACERealm，使用使用者名稱/passcode（PIN+Token code）在 ACE 伺服器上驗證身份。

例二：

- 背景

某企業爲中小型企業。使用者類型包括：區域網路路使用者、遠端存取使用者……

其中：

User1：遠端存取使用者，安全需求一般。在 LocalSever 中有使用者名稱/密碼。企業的合作

夥伴或代理商可使用這種使用者身份連入企業的內部網。

User2：Windows NT 域使用者。安全需求較高，在 Windows NT 伺服器上有使用者名稱/密碼。需要 Windows NT 域使用者名稱進行身份認證。

Group1：成員包括 User1。群組的設定可參考使用者的設定。

● 身份驗證設定

1. 預置以下幾個伺服器。

   LocalUsers：預設。不需增刪也不能更改。類型爲 Local；

   NTUsers：類型爲 Windows NT。

2. 預置以下幾個安全域。

   LocalUsers：預設。不需增刪也不能更改。

   NTRealm: 新增。需要驗證 NT domain 的使用者名稱/密碼。

| 設定項 | 値 | 說明 |
|---|---|---|
| 使用以下伺服器進行認證/制定策略 | NTUsers | 類型：Windows NT |
| 通過 Certificate/PKI 認證 | True | 選中該選項，並點選<管理證書>選擇信任的根證書。 |

3. 將使用者/群組按安全需求加入到相應的安全域中。

   User1/Group1：加入 LocalUsers。使用使用者名稱/密碼在 Local 伺服器上認證身份。驗證通過後，進行應用授權。

   User2：加入 NTRealm，通過企業的 Windows NT 伺服器驗證使用者身份。驗證通過後，進行應用授權。

## 3.3.1 添加認證伺服器和使用者

### 添加伺服器：

1 在系統主介面中（如圖 4）的“安全管理” 下，點選 認證控制。

2 點選圖 13 中的<增加/編輯伺服器>，進入圖 7 所示介面。

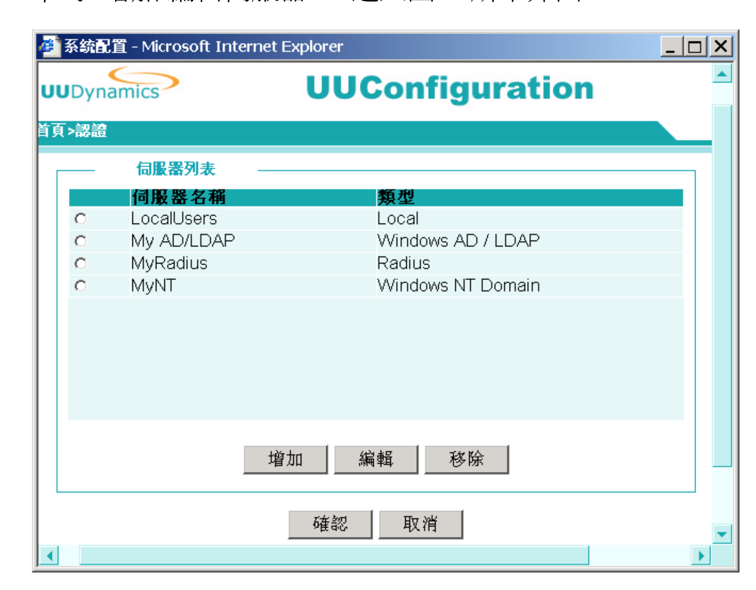



圖 7

3 點選<增加>，進入圖 8 所示介面。從“伺服器類型”列表中選擇類型，選擇不同的類型後，會出現不同的介面，填入相應的資料。各輸入項的填寫說明請參見下表。

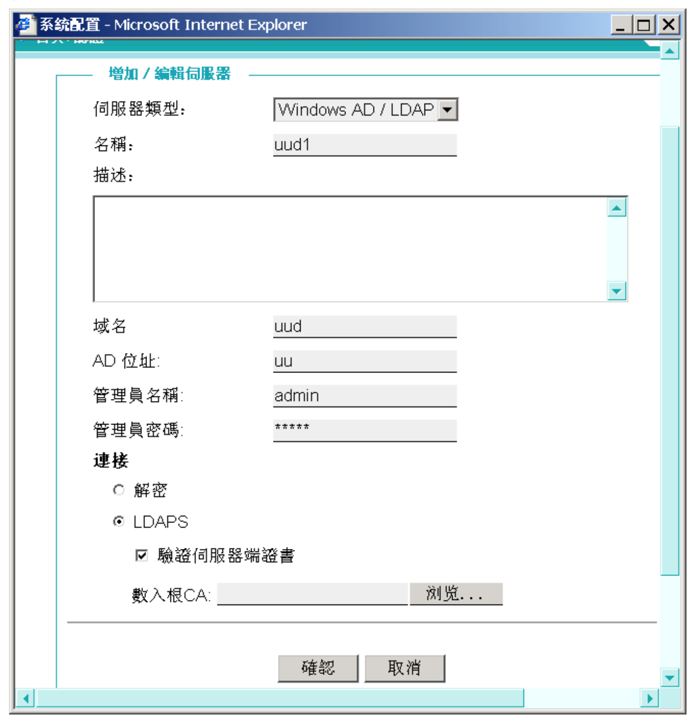



圖 8

4 設定完畢後，重復點選<確認>，直到返回圖 13 所示介面。

5 點選<生效>，保存設定。

**表：各輸入項的填寫說明**

| 伺服器 Type | 輸入項 | | 說明 |
|---|---|---|---|
| Window AD/LDAP（Window AD/NTLM） | 名稱 | | 輸入伺服器名稱 |
| | 描述 | | 輸入對該伺服器的描述（可選） |
| | 功能變數名稱 | | 輸入對應的 DNS 名稱 |
| | AD 位址 | | 輸入該域服務器的 IP 位址或功能變數名稱（Window AD/LDAP 類型中如果下面的“連接” 選項爲 LDAPS 時，必須輸入功能變數名稱） |
| | 管理員名稱/管理員密碼 | | 輸入登錄該域的管理員使用者名稱、密碼 |
| | 連接（僅 Window AD/LDAP 類型） | 解密 | 連接過程不加密 |
| | | LDAPS | 驗證伺服器端證書：選中該選項後，連接不但被加密，還需要驗證伺服器提供的證書 |
| | | | 導入根 CA：導入簽發 Certificate 的根 CA |
| LocalUsers | 名稱 | | 輸入伺服器名稱 |
| | 描述 | | 輸入對該伺服器的描述（可選） |
| | 使用者 | | 在該伺服器中增加使用者 |
| | 群組 | | 在該伺服器中增加群組 |
| LDAP（可參考表格下的實 | 名稱 | | 輸入伺服器名稱 |
| | 描述 | | 輸入對該伺服器的描述（可選） |

| 例） | 類型 | | • Active Directory;<br>• OpenLDAP;<br>• Generic LDAP with Static Groups：除了以上兩種類型之外的其他類型 |
|---|---|---|---|
| | 伺服器 | | LDAP 伺服器的 IP 位元址或名稱 |
| | 使用預設埠 | | 可選項。預設埠號爲：<br>• 不加密：389<br>• 使用 SSL 協定加密：636<br>如果沒有選中該項，則需要另行設定埠號 |
| | 授權需要經過 LDAP 搜尋 | Admin DN | 指定在 LDAP 伺服器上搜尋管理員的目錄路徑 |
| | | 密碼 | 輸入該管理員的密碼。 |
| | 指定如何找出使用者輸入 | Base DN | 指定在 LDAP 伺服器上搜尋使用者的目錄路徑 |
| | | 屬性 | 指定以哪個屬性類型（可以是 LDAP 伺服器管理員定制的屬性類型）作爲使用者名稱 |
| | | 過濾器 | 設定過濾條件 |
| | 決定群組成員 | Base DN | 指定在 LDAP 伺服器上搜尋組的目錄路徑 |
| | | 屬性 | 指定以哪個屬性類型（可以是 LDAP 伺服器管理員定制的屬性類型）作爲組名稱 |
| | | 過濾器 | 設定過濾條件 |
| | | 成員屬性 | 指定 LDAP 伺服器上的屬性類型(可以是 LDAP 伺服器管理員定制的屬性類型)，用于驗證靜態組的成員。 |
| | 連接 | 解密 | 連接過程不加密 |
| | | LDAPS | 驗證伺服器端證書：選中該選項後，連接不但被加密，還需要驗證伺服器提供的證書<br>導入根 CA：導入簽發 Certificate 的根 CA |
| Radius | 名稱 | | 輸入伺服器名稱 |
| | 描述 | | 輸入對該伺服器的描述（可選） |
| | Radius 伺服器 | | 輸入 Radius 伺服器的 IP 位址 |
| | Radius 埠 | | 輸入 Radius 伺服器的埠 |
| | Shared Key | | 輸入 Shared Key |
| ACE/Server | 名稱 | | 輸入伺服器名稱 |
| | 描述 | | 輸入對該伺服器的描述（可選） |
| | 導入至 | | 導入.REC 文件後，系統自動記錄并回顯導入的時間 |
| | 導入新的配置檔 | | 將相應的 .REC 文件導入。該文件由 ACE 伺服器分配。 |
| | 刪除節點 Secret | | 用於和 ACE/Server 端的同步。如果在某一端刪除了節點 Secret，必須在另一端也相應刪除。 |

舉例：LDAP 類型伺服器的目錄如下

dc= qa,dc=com
    Ou=people
        Uid=tester1
        Uid=tester2
    Ou=group
        Cn=test
        Cn=test1

說明：
管理員 DN：cn=root,dc=qa,dc=com
使用者 屬性：cn；
過濾: objectclass=person
組成員 屬性：cn；
過濾: objectclass=posixgroup,
成員屬性：MemberUid

（test、 test1 爲群組。tester1、 tester2 爲使用者，配置見圖 9）

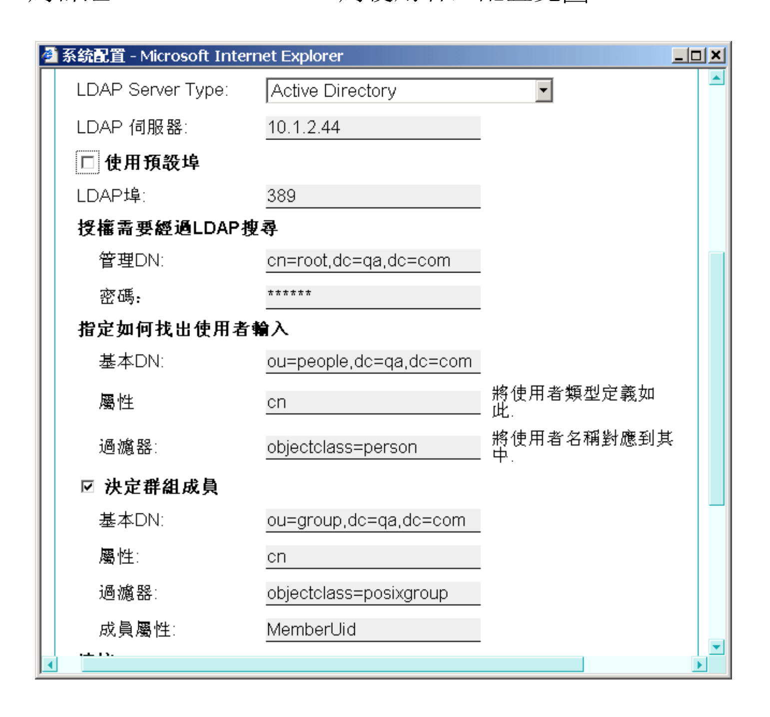



圖 9

📖 說明：

- **Windows AD/LDAP** 伺服器與 **Windows AD/NTLM** 伺服器比較

前者有三條限制：

1. Windows AD/LDAP 方式下，“名稱”欄內填入的名稱必須與下一欄所指定 IP 的伺服器中存在的 AD 名稱一致。
2. Windows AD/LDAP 方式下，僅能搜索出 1000 條以下的“遠端管理員”記錄（有關搜索遠端管理員記錄的內容請參考“3.3.5 設定本地（/遠端）管理員”）。
3. Windows AD/LDAP 方式下，在對應的 Windows AD 域中增加的組可能需要 20 分鐘後才能生效。增加的組包括“新增的新組”和“刪除後增加的同名稱組”。該組中的使用者如果無法登錄 UU100，請稍候再試。

- **LocalUsers** 伺服器

LocalUsers 是預設的伺服器類型。如果選擇 LocalUsers 類型的伺服器，則表示選擇在 UU100 中單獨建立一個使用者認證檔案。這個檔案是經過加密保護的。換言之，使用者應使用本系統定義的帳戶和密碼連入。該伺服器中有預設的使用者/密碼：admin/admin。預設的使用者 admin、伺服器和安全域不能被刪除。這樣可以保證至少有一位具有“唯讀/更改”許可權的使用者存在。

## 添加用戶：

- 僅使用證書的認證方式，不需要添加使用者。使用者存取 UU100 時，僅需提供證書即可。
- 在添加 LocalUsers 伺服器時，可以通過點選<使用者>添加使用者，并設定密碼。
- 在添加其他類型伺服器時，只要按照表格中的說明塡寫各輸入項，UU100 會自動到指定的認證伺服器獲取該伺服器中的符合條件的使用者列表。這種結合現有的認證伺服器進行用戶認證的方式，使得企業可以使用統一的安全認證策略，無需另外添加用戶。

## 3.3.2 添加證書

1. 在系統主介面中（如圖 4）的“安全管理” 下，點選 認證控制。
2. 點選圖 13 中的<增加/編輯根證書>。在介面中點選<增加>，在下圖所示介面中輸入相應的證書資訊。
   “證書約束條件”欄用于輸入證書的限制規則。其語法結構爲：
   [*系統變數名稱*].[*屬性名稱*]＋[*操作符*]＋[*屬性値*]（或另一 [*系統變數名稱*].[*屬性名稱*]）。
   舉例：
   ①Certattr.CN ='Zhang san'含義爲：證書中 CN 必須爲 Zhang san。
   ②Certattr.CN =User.name 含義爲：證書中 CN 必須和登錄時所用的使用者名稱一致。

   **說明：**
   ***i*STAR™**定義了三類系統變數：User 類、Userattr 類、Certattr 類。其中，
   **User** 類包括 name、groupname 屬性。User.name 表示登錄時所用的使用者名稱，User.groupname 表示該使用者名稱所屬的群組。
   **Userattr** 類 包括：Service-Type、Framed-IP-Address、Framed-IP-子網掩碼等用戶屬性。
   **Certattr** 類 包括：C,CN,L,O,OU,Email 等證書的屬性。
   操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。
3. 設定完畢後，重復點選<確認>，直到返回圖 13 所示介面。
4. 點選<生效>，保存設定。

## 3.3.3 添加角色

如果認證伺服器指定的是“None” （僅使用 PKI）或“Radius”類型的伺服器，則還需要預先定義角色。以便設定規定將相應的角色與 Radius 伺服器或證書中的用戶對應起來（見圖 14）。

1. 在系統主介面中（如圖 4）的“安全管理” 下，點選 認證控制。
2. 在圖 13 所示介面，點選<增加/編輯角色>。開啓圖 10 所示介面。
3. 點選<新建>，進入圖 11 所示介面。輸入角色名稱。




圖 10

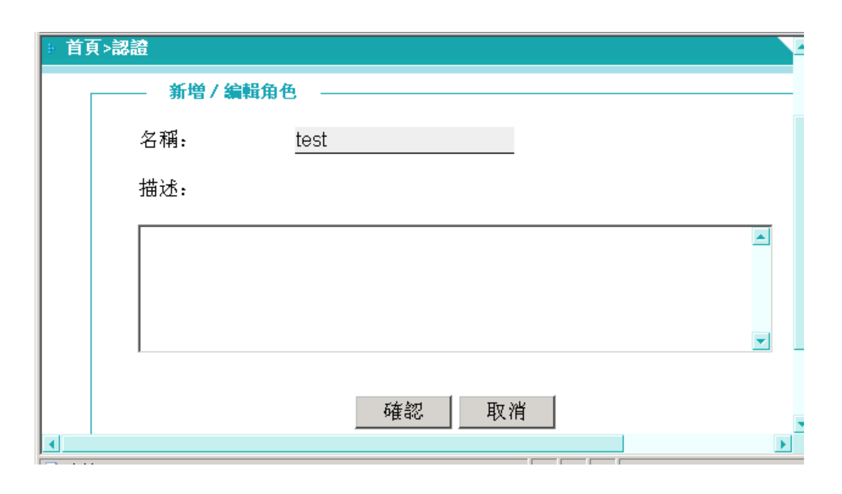



圖 11

4. 設定完畢後，重復點選<確認>，直到返回圖 13 所示介面。
5. 點選<生效>，保存設定。

### 3.3.4 添加安全域

添加安全域之前，應預先準備必須的伺服器、角色或證書等。準備的流程可參考下圖：

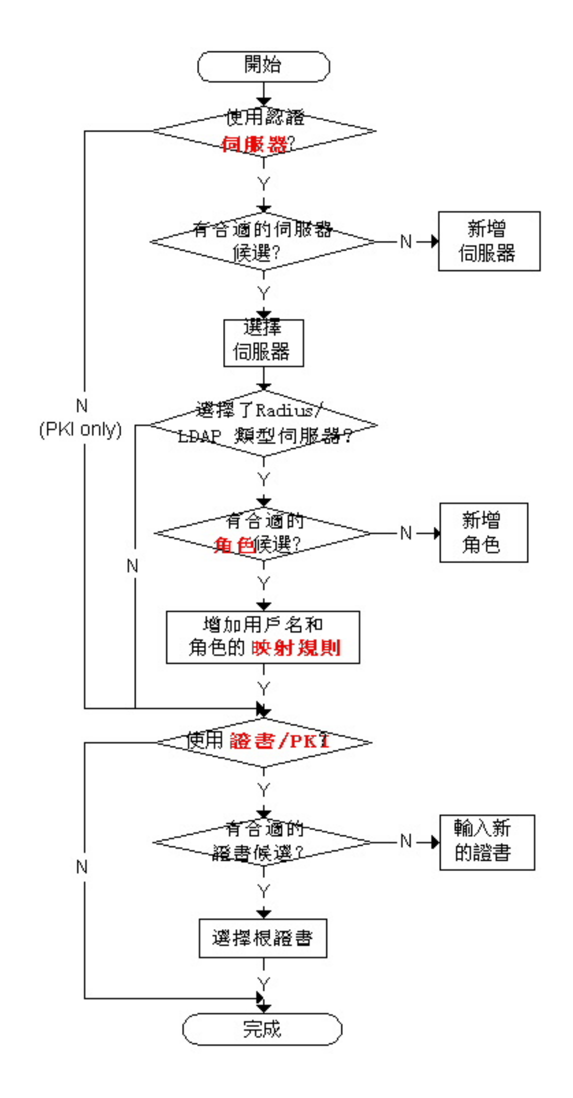



圖 12 設定流程圖

1. 在系統主介面中（如圖 4）的“安全管理” 下，點選 認證控制。




圖 13

2. 在圖 13 所示介面上點選<增加>，可以增加新的安全域。

   選中列表中某個安全域，點選<編輯>，可以修改該安全域的屬性。

3. 輸入或修改安全域的名稱。如果需要對該安全域進行描述，請在“描述”欄內輸入說

明性文字。

例如圖 14 中，安全域名稱：RadiusUsers。

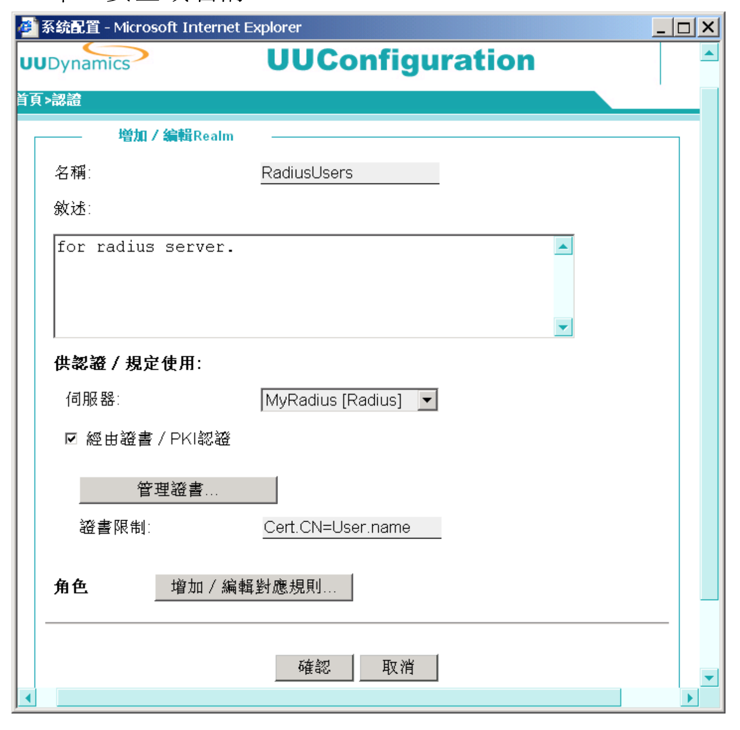



圖 14

4. 在“伺服器”欄選擇需要在哪個伺服器上進行使用者身份驗證。例如圖 14 中，選擇伺服器 MyRadius。在列表中選擇伺服器後，則直接轉至下一步繼續其他操作。但是如果列表中沒有您所需要的伺服器，請先添加伺服器。
5. 如果需要驗證 Client 端使用者提供的證書，請勾選“通過 Certificate/PKI 認證”。否則，直接跳轉至下一步（步驟 7）。
   點選<管理證書>，可以選擇已有的證書。如果沒有需要的證書，請先添加合適的證書。
6. 如果認證伺服器指定了除 “None”（僅使用 PKI）或“Radius”兩種類型之外的其他類型伺服器，跳轉至步驟 9。
   如果認證伺服器指定的是“None” （僅使用 PKI）或“Radius”類型的伺服器，則還需要爲角色設定相應的規則（見圖 14）。
7. 在圖 14 所示介面中點選<增加/編輯映射規則…>，進入所示圖 15 介面。

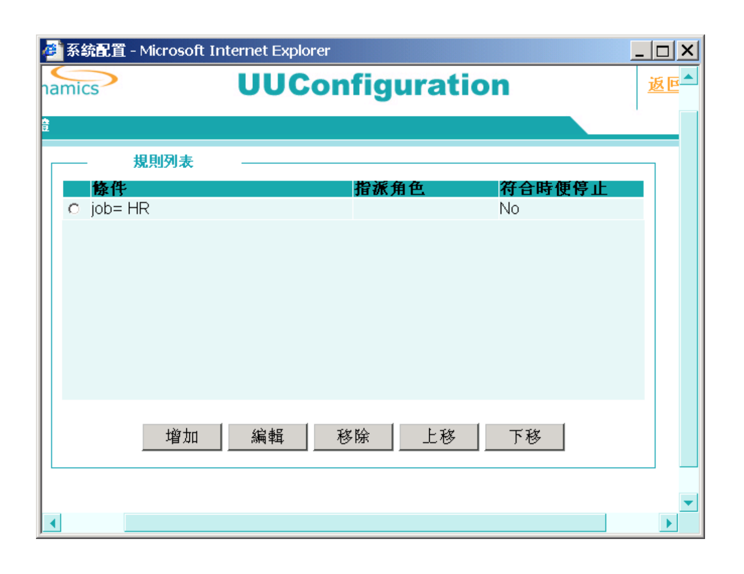



圖 15

以 Radius 伺服器爲例：

點選圖 15 介面上的<增加>，進入圖 16 所示介面增加新的規則。

增加規則的內容包括：根據 Radius 伺服器中的使用者屬性，設定過濾條件，篩選出所有的符合條件的使用者，然後將這些使用者歸入某一角色中。這樣，當對某個角色進行授權或其他操作時，實際上是對所有符合規則中過濾條件的使用者同時進行操作。其語法結構爲：

[*系統變數名稱*].[*屬性名稱*]＋[*操作符*]＋[*屬性值*]（或另一 [*系統變數名稱*].[*屬性名稱*]）。

舉例：

①圖 16 中的規則含義爲：Radius 伺服器中所有屬性 service-type 取值爲 framed-user 的使用者都屬於角色“admin”。

②Certattr.CN =User.name 含義爲：證書中 CN 必須和登錄時所用的使用者名稱一致。

🕮 說明：

***i*STAR™**定義了三類系統變數：User 類、Userattr 類、Certattr 類。其中，

**User** 類包括 name、groupname 屬性。User.name 表示登錄時所用的使用者名稱，User.groupname 表示該使用者名稱所屬的群組。

**Userattr** 類 包括：Service-Type、Framed-IP-Address、Framed-IP-子網掩碼等用戶屬性。

**Certattr** 類 包括：C,CN,L,O,OU,Email 等證書的屬性。

操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。

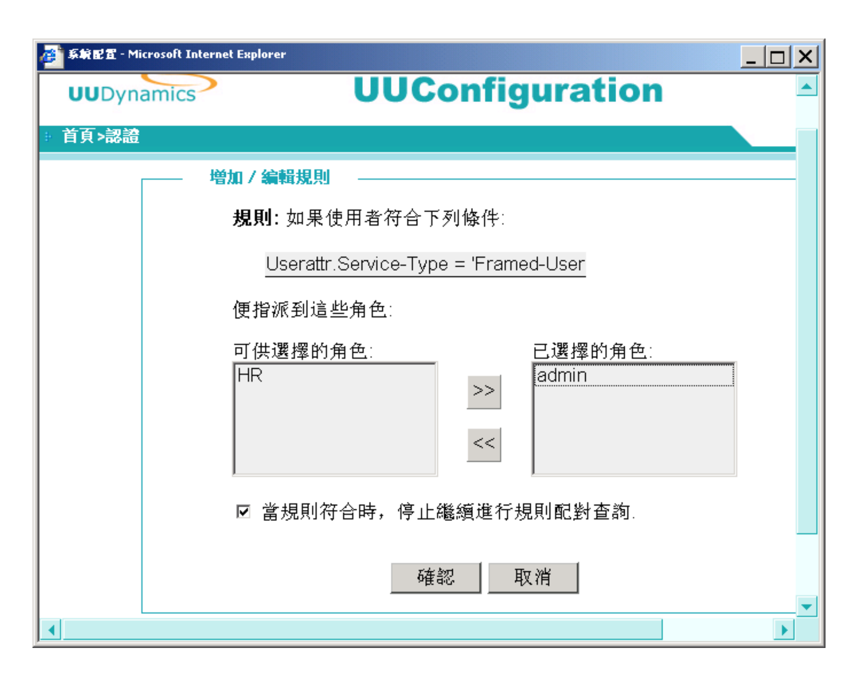



圖 16

8. 設定完畢後，重復點選<確認>，直到返回圖 13 所示介面。
9. 點選<生效>，保存設定。

### 3.3.5 設定本地（/遠端）管理員

在系統主介面中（如圖 4）的“安全管理”之下，按下本地管理會出現如圖 17 的視窗；用以增加或移除本地系統管理員。按下 遠端管理 會出現如圖 18 的視窗；用以增加或移除遠端系統管理員。

ⓘ 注意：

1. 在本地管理 中添加的使用者爲本地管理員，能且僅能從本機登入 UU100 系統管理介面。
2. 在遠端管理 中添加的使用者，遠端系統管理員必須首先是本地管理員，即必須先在 本地管理 中加入該使用者名稱。

- 本地管理：

1. 如圖 17，本地管理員對 UU100 的訪問策略爲“拒絕”，意即使用者列表中所有的使用者都不能訪問。
2. 在“使用者列表”選項組中選擇使用者類型爲“使用者”或是“群組”。在選項組下的“使用者列表”列表中勾選可以通過本地方式存取 UU100 的使用者（/組），並按<增加>將其加入下方的“除了以下列出的”目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者（/組/角色）。
3. 在“訪問類型”中設定該管理員的權限。各種許可權的含義分別爲：
   唯讀:表示該使用者對系統管理介面有“唯讀”許可權。
   更改:表示該使用者對系統管理介面有“唯讀”、“修改”和“使更改生效”的許可權。
4. 以上步驟完成後，點選<生效>保存設定結果，幷返回到圖 4 系統主介面。

- 遠端管理：

1. 如圖 18 所示，爲保證管理員遠端管理時建立的 SSL 連接的安全，您可以設定允許會話持續的最長時長和允許會話空閑的最長時長。超過設定的時長，系統會自動斷開這次連接。
2. 如果勾選“允許同一使用者多次訪問”， 則同一管理员再次（或使用同樣的使用者名稱從其他機器）獲取管理專案列表時，不影響之前以該使用者名稱獲取管理專案列表的其他會話。

   反之，如果不勾選該選項，則登入時會强行中止之前的所有以該使用者名稱獲取管理專案列表的會話。
3. 選擇需要進行遠端管理的應用服務，點選<編輯>，進入圖 19 所示介面。
4. 設定是否對該服務使用加密、哈希以及壓縮演算法。
5. 點選<規定>設定，設定該服務使用哪一個證書驗證遠端管理員身份。
6. 點選<使用者>設定該服務的遠端管理者。
7. 如圖 21 所示，將遠端管理員所屬的安全域從“可選擇”列表框中移至“已選定”列表框（設定本地管理員時，該步驟不需要）。如果選擇的是包含有角色角色資訊的 Radius 或 PKI 類型的安全域，會顯示圖 22 所示的操作介面。
8. 設定該管理員對 UU100 的訪問策略，系統預設的是“拒絕”，意即所有的管理員都不能訪問。
9. 在“使用者列表”中指定排除在訪問策略之外的方式。在其下的“使用者列表”列表中勾選使用者（/組/角色）方式，並按<增加>將其加入下方的“除了以下列出的”目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者（/組/角色）。

   通過這一步驟結合設定訪問策略步驟相結合，管理員可以靈活的設定訪問許可權，即：僅允許某一些管理員訪問，或者允許除某一些管理員外的所有管理員訪問。

   在“使用者列表”中指定排除在存取策略之外的方式。在其下的“使用者列表”列表中勾選使用者（/組/角色）方式，並按<增加>將其加入下方的“除了以下列出的”目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者（/組/角色）。

   如果安全域指定的伺服器類型爲“Windows AD/LDAP”，同時该服务器中的“管理員名稱”中輸入的管理員屬於該域的“Domain Admins”組，則圖 21 中的“使用者列表” 列表將顯示該域中所有的使用者，否則，圖 21 中的“使用者列表” 列表只能顯示該域中的部分使用者。
10. 如果在圖 21 的視窗中的空白欄輸入要搜索的字串幷點選<搜索/開始>，介面上將返回模糊查詢後的結果。圖中顯示了對“test”搜索的結果。（是否有搜索功能與伺服器的類型有關。）
11. 在“訪問類型”中設定該管理員的權限。各種許可權的含義分別爲：

    唯讀:表示該使用者對系統管理介面有“唯讀”許可權。

    更改:表示該使用者對系統管理介面有“唯讀”、“修改”和“使更改生效”的許可權。
12. 以上步驟完成後，保存設定結果，幷返回到圖 4 系統主介面中。

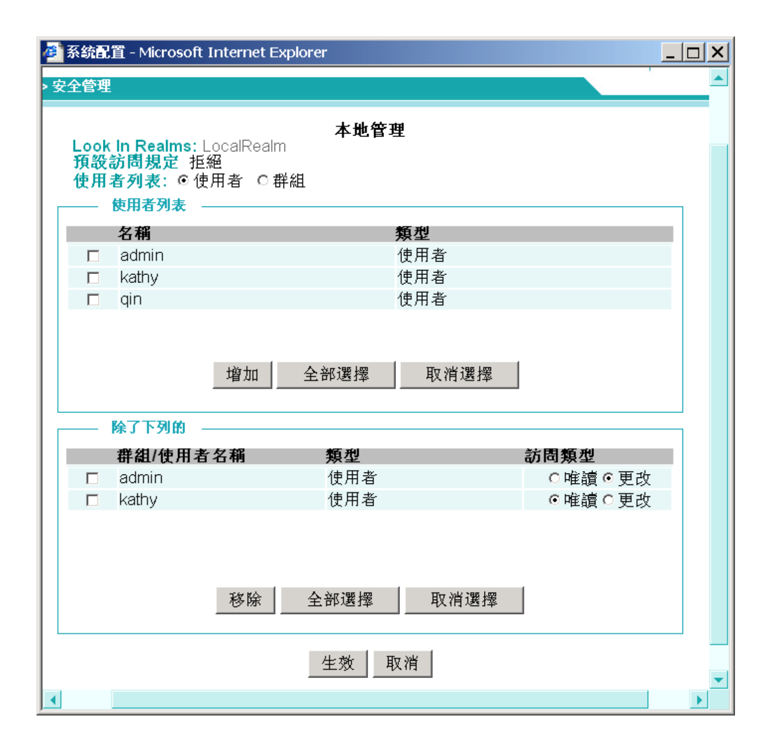

系統配置 - Microsoft Internet Explorer
安全管理
本地管理
Look In Realms: LocalRealm
預設訪問規定 拒絕
使用者列表: 使用者 群組
使用者列表
名稱
類型
admin
使用者
kathy
使用者
qin
使用者
增加
全部選擇
取消選擇
除了下列的
群組/使用者名稱
類型
訪問類型
admin
使用者
唯讀 更改
kathy
使用者
唯讀 更改
移除
全部選擇
取消選擇
生效
取消

圖 17

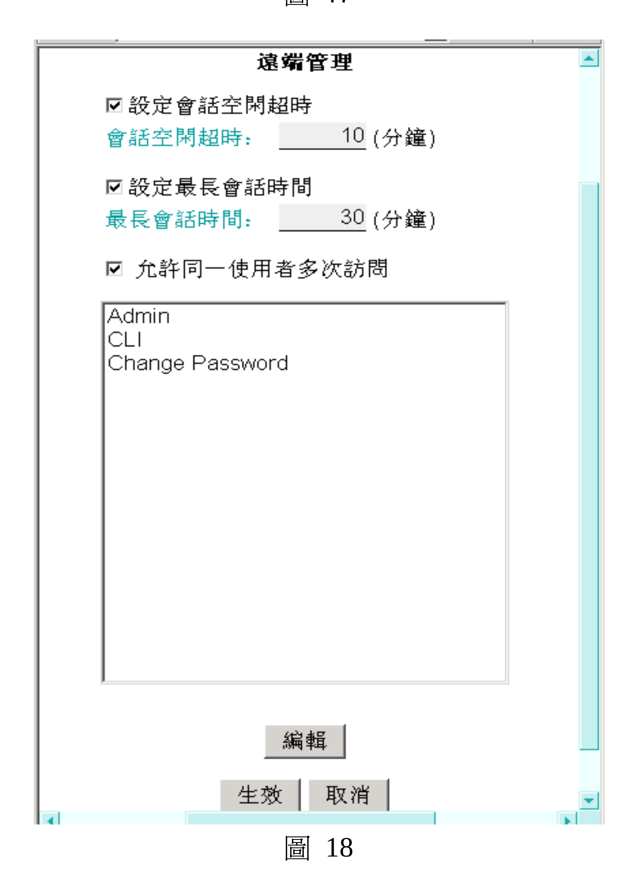

遠端管理
設定會話空閑超時
會話空閑超時: 10 (分鐘)
設定最長會話時間
最長會話時間: 30 (分鐘)
允許同一使用者多次訪問
Admin
CLI
Change Password
編輯
生效
取消

圖 18

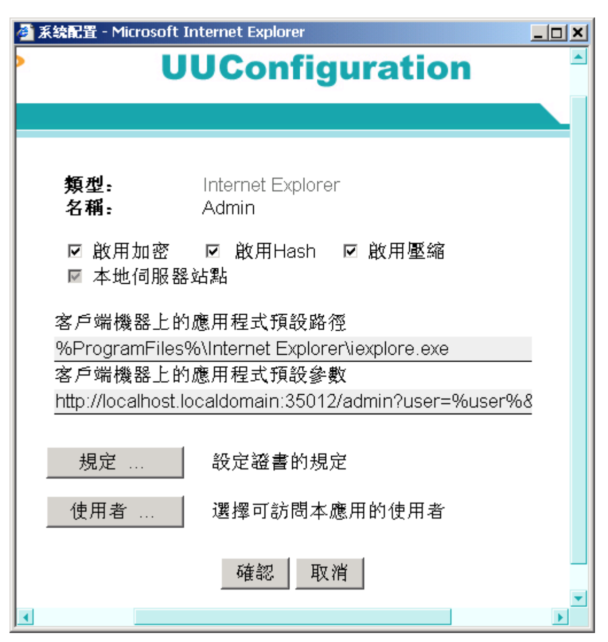

系統配置 - Microsoft Internet Explorer
UUConfiguration
類型: Internet Explorer
名稱: Admin
啟用加密
啟用Hash
啟用壓縮
本地伺服器站點
客戶端機器上的應用程式預設路徑
%ProgramFiles%\Internet Explorer\iexplore.exe
客戶端機器上的應用程式預設參數
http://localhost.localdomain:35012/admin?user=%user%
規定 ...
設定證書的規定
使用者 ...
選擇可訪問本應用的使用者
確認
取消

圖 19


系統配置 - Microsoft Internet Explorer
Dynamics
UUConfiguration
>認證
新增 / 編輯發佈規定
名稱:
Admin
經由證書 / PKI認證
確認
取消

圖 20


遠端管理
可供選擇
MyRadius
已選擇
LocalRealm
My AD/LDAP Realm
> >
< <
設置使用者和群組的權限
預設訪問規定 拒絕 允許
使用者列表: 使用者 群組
使用者列表
名稱
類型
admin 使用者
kathy 使用者
qin 使用者
增加
全部選擇
取消選擇
除了下列的
群組/使用者名稱
類型
admin 使用者

圖 21




圖 22

## 3.3.6 不同用戶存取 UU100 的方法

- 使用者

使用者通常從遠端存取 UU100，并訂閱 UU100 所發布的的各類應用。仅具有使用者号的用户是不能管理 UU100 的。

多個不同的使用者可以同時獲取應用列表。同一使用者可以多次獲取應用列表，前提是 發布應用中勾選了“允許同一使用者多次訪問”。

例如：

- 不同使用者名稱的使用者可以同時獲取應用列表。
- 不同安全域中同名的使用者可以同時獲取應用列表。
- 管理員在發布應用時勾選了“允許同一使用者多次訪問”，則相同安全域中同名的使用者可以同時獲取應用列表。
- 管理員在發布應用時沒有勾選“允許同一使用者多次訪問”，則相同安全域中同名的使用者獲取應用列表時。會將原已連入的會話斷開。

獲取應用列表的方式：通過 IE 瀏覽器，使用者可以在任何一台聯機到網際網路的電腦上輸入：

https://[uuswitch （/uuexchange的DNS名稱或IP位址）/[uu100UUID]

- 本地管理員

本地管理員僅能從本機存取 UU100，通過身份驗證後，登入 UU100 進行管理。任何時候，只能有一位管理員登入。如果之前未正常登出或已有其他管理員登入，需要先將原登入者停掉。詳細說明請參考“3.2.3 退出設定介面”。 但是多個不同的管理員可以同時獲取管理專案列表，前提是 遠端管理 中勾選了“允許”。

例如：

不同使用者名稱的管理員可以同時獲取管理專案列表。

不同安全域中同名的管理員可以同時獲取管理專案列表。

但是，相同安全域中同名的管理員不可以同時獲取管理專案列表。必須將原已連入的管理員停掉。這樣原已連入的會話會斷開。

獲取管理專案列表的方式：在本機熒幕右下角的應用程式托盤處，點擊滑鼠右鍵，點選“配置”，顯示以下的視窗。輸入正確管理員名稱、密碼。即可登入。

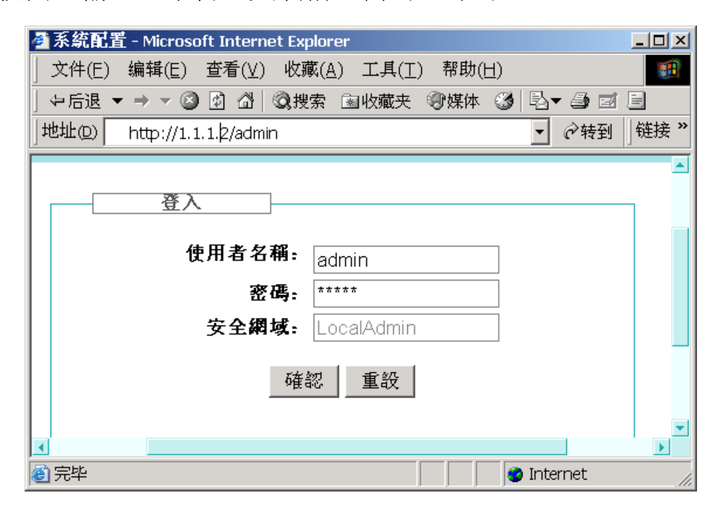



圖 23

- 遠端管理員

遠端管理員僅能從遠端存取 UUSwitch（/UUExchange），通過身份驗證後，登入 UUSwitch（/UUExchange）進行管理。

獲取管理專案列表的方式：通過 IE 瀏覽器，遠端系統管理員可以在任何一台聯機到網際網路的電腦上輸入：

https://[uuswitch（/uuexchange的DNS名稱或IP位址）/[uu100UUID]/rm

顯示以下的視窗：

用户认证信息
发布单元: localhost
安全域: localadmin
用户名: admin
密码:
高級
证书: NULL
Session 清理 配置
确定 取消

圖 24

在圖 24 所示介面中輸入身份認證所需要素，點選<確定>之後，可獲取管理專案列表（如圖 25 視窗），遠端系統管理員啓動“Admin”圖示，輸入對應的管理員帳號和密碼，出現圖 23 所示介面。輸入使用者名稱和密碼，便可以對 UU100 進行遠端管理。如果 Admin 等服務需要證書驗證身份，則還需在圖 26 所示介面中選取正確的證書。

任何時候，只能有一位管理員登入管理介面。如果之前未正常登出或已有其他管理員登入，需要先將原登入者停掉。詳細說明請參考“3.2.3 退出設定介面”。 但是多個不同的使用者可以同時獲取應用列表。同一使用者也可以多次獲取應用列表，前提是 遠端管理 中勾選了“允許同一使用者多次訪問”。

例如：

- 不同使用者名稱的管理員可以同時獲取管理專案列表。
- 不同安全域中同名的管理員可以同時獲取管理專案列表。
- 管理員在發布應用時勾選了"允許同一使用者多次訪問"，則相同安全域中同名的管理員可以同時獲取管理專案列表。
- 管理員在發布應用時沒有勾選"允許同一使用者多次訪問"，則相同安全域中同名的管理員獲取應用列表時。會將原已連入的會話斷開。

📖 說明：

- 如果身份認證在 LocalRealm 上進行，則僅需要輸入 LocalRealm 中的使用者名稱及密碼。
- 如果認證在 ACE 伺服器上進行，則請輸入 ACE 伺服器上的使用者名稱及密碼，並在密碼後接著輸入 Token code。(當 Token 的顯示幕顯示的六格短橫杠僅剩一格時，說明該 token code 即將失效，此時請等待 ACE 伺服器分配下一個 code，並輸入這個新的 code。
- 如果認證在其他類型的安全域中進行，則需要輸入相應認證伺服器中的使用者名稱及密碼。
- 如果在安全域進行認證需要核實 Certificate/PKI，則需要勾選"高級"，並在"證書"欄選擇證書。在安全域中使用的證書與上面提及的 Admin、CLI、Change Password 等服務中使用的證書可以不一樣。

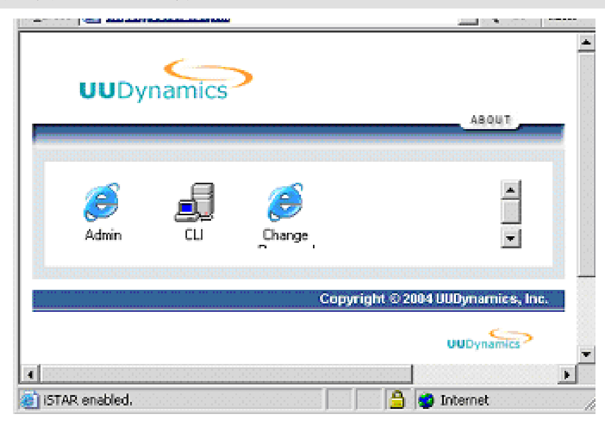



圖 25

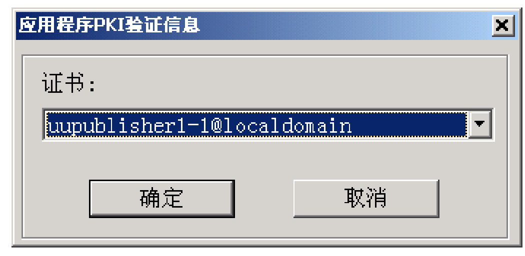



圖 26

在圖 24 所示介面中，勾選"Session 清理"。將會將電腦中的各種與該使用者相關的暫存檔案、cookies 等資訊刪除。點選<高級>可以指定要清理的專案。系統將在 Session 結束後立即清空，並且不能撤銷，請謹慎操作。

📖 說明

使用者使用共用電腦（如網吧電腦）連入 UU100 時，可以考慮此功能，以保護個人資訊

安全。

| 設定項 | 說明 | 位置 |
|---|---|---|
| Internet 瀏覽暫存 | 清除 Cache 中該使用者的所有臨時的 Internet 檔 | [*系統盤符*]:\Documents and Settings\[*username*]\Temporary Internet Files |
| Internet 瀏覽歷史記錄 | 清除 IE 中所有的瀏覽頁面的歷史記錄 | |
| Internet Cookies | 清除 IE 中的所有 Cookies | [*系統盤符*]:\Documents and Settings\[*username*]\Cookies |
| 鍵入的 URL | 清除 IE 位址欄裏的所有的 URL 記錄 | |
| 自動填充表格 | 清除 IE 上所有表單中自動填充部分的內容 | |
| 自動填充密碼 | 清除所有自動填充的密碼 | |
| Internet 收藏 | 清除該使用者在 IE 收藏夾裏的所有內容 | [*系統盤符*]:\Documents and Settings\[*username*]\Favorites |
| 暫存檔案 | 清除所有的暫存檔案 | |
| Telnet 歷史記錄 | 清除該使用者在本機上所有的 Telnet 記錄 | |
| 垃圾箱 | 清空系統盤符下的垃圾箱 | |
| 運行歷史記錄 | 清除 Windows“開始->程式”功能表中的最近運行程式的記錄列表 | [*系統盤符*]:\Documents and Settings\[*username*]\Start Menu\Programs |
| 最近的文檔 | “開始->文檔”功能表中的最近開啓文檔的記錄列表 | [*系統盤符*]:\Documents and Settings\[*username*]\Recent |
| 最後登入使用者 | 清除上一次登入的使用者名稱 | |
| 查找文件歷史記錄 | 清除上一次查找檔的搜索結果 | |
| 查找電腦歷史記錄 | 清除上一次查找電腦的搜索結果 | |
| 網路歷史記錄 | 清除“網路芳鄰”中所有的映射目錄 | [*系統盤符*]:\Documents and Settings\[*username*]\NetHood |

# 3.4 網路設定

## 3.4.1 設定網路環境

如圖 4，點選“網路設置”下的 網路設置，進入圖 27 的介面。

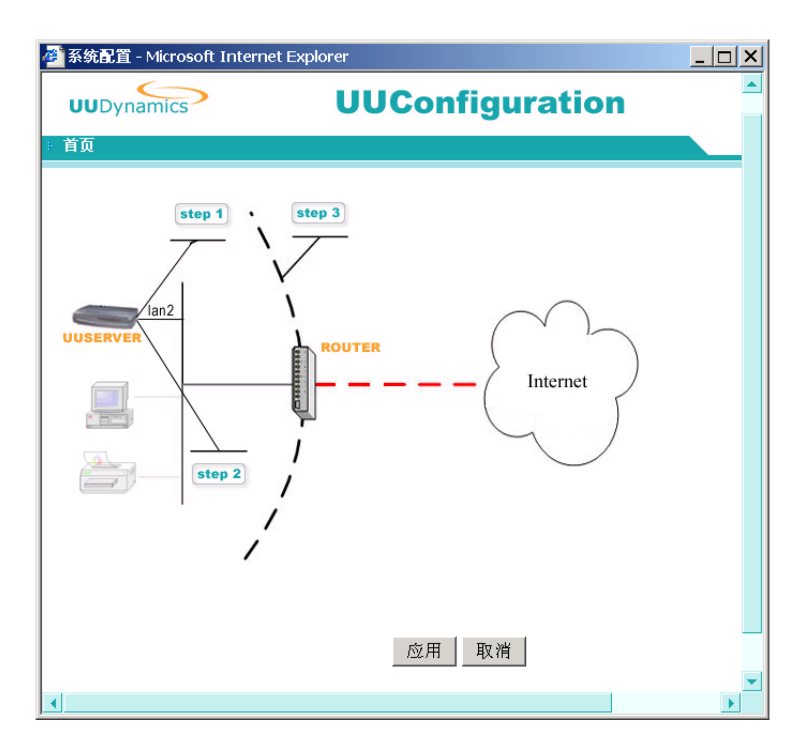



圖 27

① 點選 “步驟 1”進入圖 28 所示介面。其中，“訪問類型”表示 UU100 接入網路的類型：

- ◆ 選 “STATIC” 時，選擇本台電腦的 “轉接器名稱” 。UU100 的 IP 位址、對應的子網掩碼、閘道及 DNS 等參數會自動從系統讀取。按<保存>。如圖 28 所示。




圖 28

- ◆ 選 “DHCP” 時（當需要對本台機器動態分配 IP 時適用），點選<保存>。此類型只在 Private Access 方式下出現。
- ◆ 選 “STATIC/PORT FORWARDING” 時（當從防火牆上 port forwarding 到該台 UU100 時使用），選擇本台電腦的 “轉接器名稱” ，系統讀取本台 UU100 的私有 IP 位址、對應的子網掩碼、閘道及 DNS 等參數，此外還要輸入 DNAT IP（如圖 29 所示），即配置 NAT 的源位元元元址。請參考下例。

此類型只在“Direct　Access”方式下出現。

例如：

UU100 放置在區域網路內。該區域網路的防火牆有兩個 PUBLIC IP：61.***.**.1 和 61.*.*.2。防火牆裏的埠對應設定爲：61.***.**.2⇔192.168.1.1。則 DNAT IP 應設定爲 61.***.**.2。但是，如果該區域網路的防火牆僅有一個 PUBLIC IP：61.***.**.1，則 DNAT IP 應設定爲 61.***.**.1。

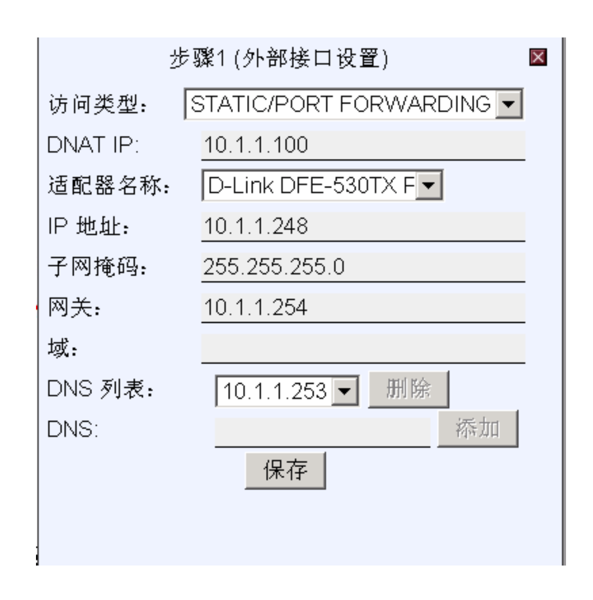



圖 29

② 點選“步驟 2”進行 Cluster 的設定。勾選“啓用 Cluster”表示啓用 Cluster。

③ 點選“步驟 3” 進入圖 30 所示介面，進行 Proxy 的設定。

系統預設無 Proxy；這裏的 Proxy 設定和 IE 的 Proxy 設定相似，支援的 Proxy 的選項有 No Proxy（表示沒有 Proxy,使用 NAT 或 Public IP 直接上網）、Web（表示有 Web Proxy）、SOCK4（表示有 SOCK4 Proxy）、SOCK5（表示有 SOCK5 Proxy）、AutoDetect（表示自動查找 Proxy 設定）和 config Script（根據 config Script 來設定 Proxy）。




圖 30

④ 完成以上操作後按<生效>，使當前的網路設定生效。系統會出現如下資訊提示框（圖

31），表示初次配置已經完成。

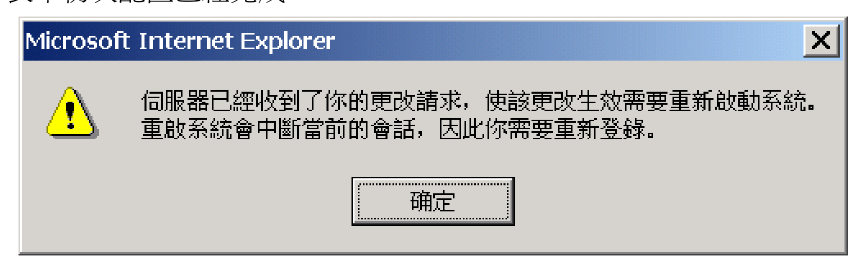



圖 31

## 3.4.2 設定連接方式

在圖 4 所示介面中，點選“網路設置”下的 iSTAR 設置。設定連接方式。

● Direct Access 方式

該方式下，遠端使用者可以通過 UU100 的公共 IP 位址直接訪問該台 UU100 所發布的應用或對它進行遠程管理。訪問應用時，在用戶端的 IE 5.0（或以上）的地址欄輸入“*https://[uu100 的公共 IP 位址]*”。如果要進行遠端管理，則輸入“https://[*uu100 的公共 IP 位址*]/rm”。

這種連接方式需要導入一個第三方數位電子憑證，或使用預設的由 UUDynamics 公司簽名的數位電子憑證，驗證接入安全

1. 在圖 32 所示介面上，點選倒三角鍵下拉功能表，選擇“Direct Access”連接方式。
2. 如果您需要導入準備好的第三方的證書。請點選<輸入>鍵，輸入該證書對應的 Key 文件，證書文件和 CA 的證書文件，所有文件要求是 Base64 編碼方式，如圖 33 所示。

> 🕮 說明：
> 有關第三方數位電子憑證的說明及獲取途徑請參見《安裝手冊》的“術語表”章節。

3. 最後按<生效>鍵，使當前的連接方式設定生效。

● Private Access 方式

該方式下，UU100 與 UUSwitch（/UUExchange）相連，幷在啓動時使用該交換單元分配的唯一的有效邏輯標識（即 UUID 檔案）註冊到交換單元。用戶端經過交換單元定位幷連接該 UU100。

因此，Private Access 優於 Direct Access 之處在於：該方式下，UU100 本身可以沒有公共靜態 IP 位址。遠端使用者只需通過交換單元的公共靜態 IP 位址和發布單元的 UUID 即可訪問連入它的各台 UU100。

訪問應用時，在用戶端的 IE 5.0（或以上）的地址欄輸入“https://[*uuswitch 或 uuexchange 的 DNS 名稱/IP 位址*]/[uu100 的 UUID]”。如果要進行遠端管理，則輸入“https://[*uuswitch 或 uuexchange 的 DNS 名稱/IP 位址*]/[uu100 的 UUID]/rm”。

> 🕮 說明：
> 對于這兩種連接方式和 UUID 的更詳細說明，請參見《安裝手冊》的“術語表”章節。

1. 在圖 32 所示介面上，點選倒三角鍵下拉功能表，選擇

"UUSwitch/UUExchange" 。

2. 導入 UUID 檔案，輸入 UUSwitch/UUExchange 的 IP 位址或 DNS 名稱。(這裏的 UUID 檔案由在這裏輸入的 UUSwitch/UUExchange 產生得到)，如圖 34、圖 35。
3. 最後按<生效>鍵，使當前的連接模式設定生效。

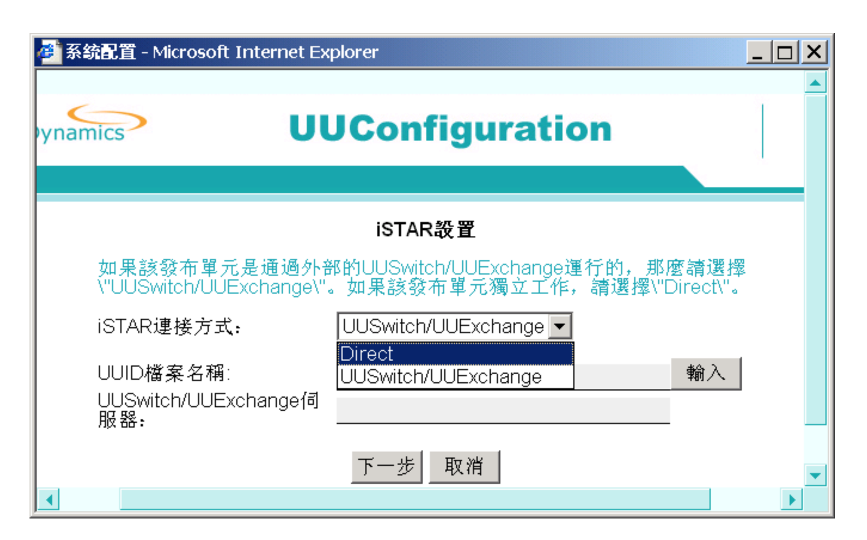



圖 32

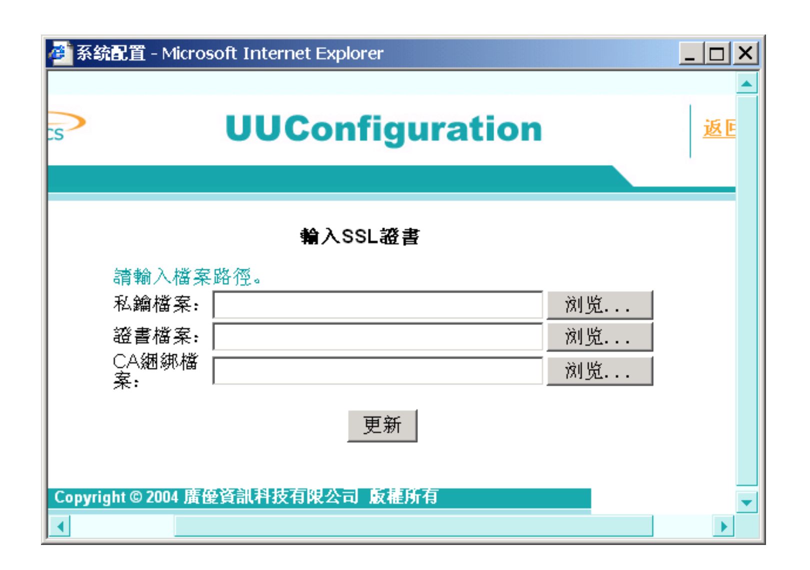



圖 33

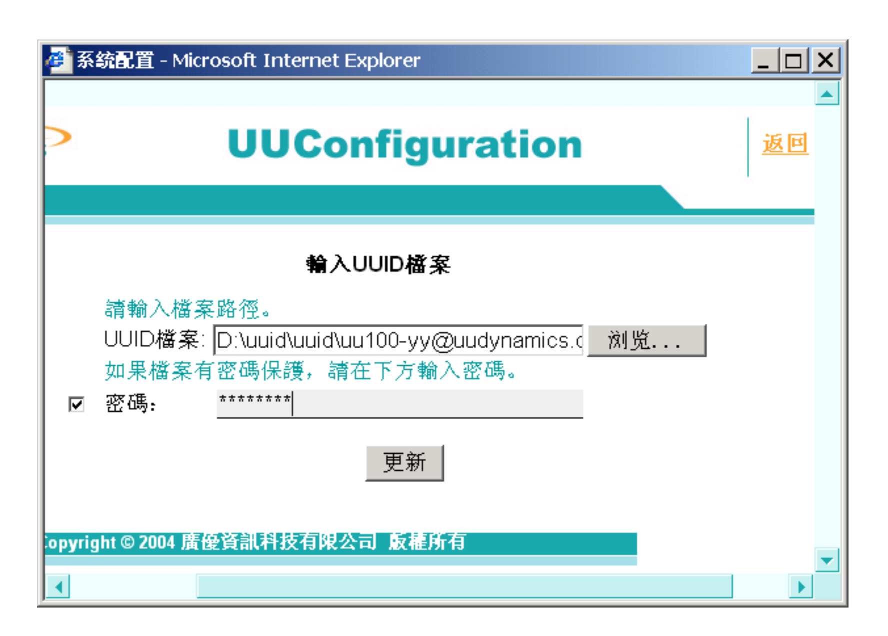



圖 34

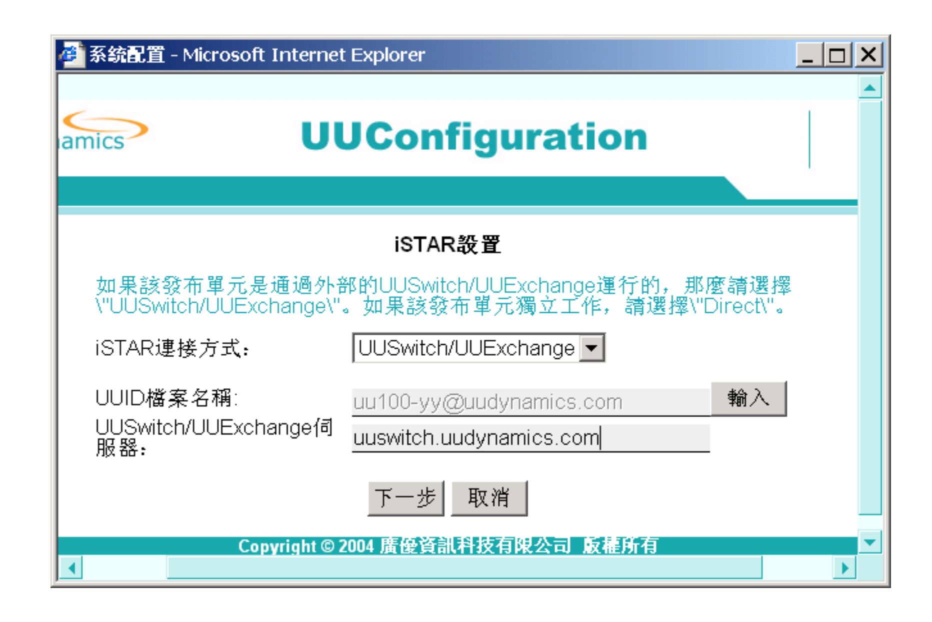



圖 35

# 3.5 安全管理

## 3.5.1 設定加密演算法

在系統主介面中（圖 4）的“安全管理”下，按下加密管理，會出現如圖 36 的視窗；用來選擇對資料的加密演算法和哈希演算法，以確保資料傳輸的安全。

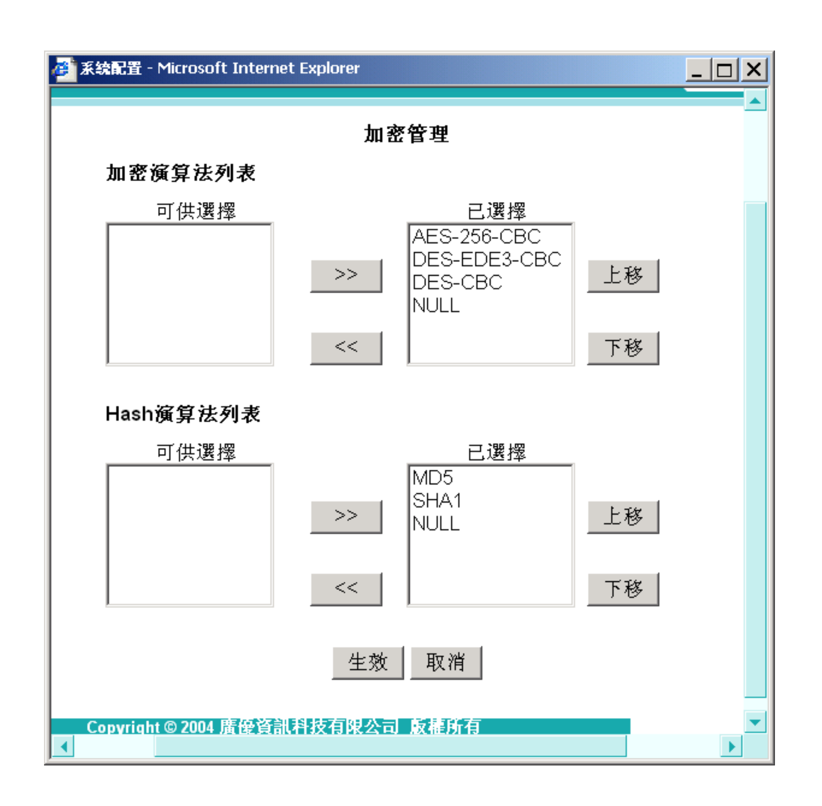



圖 36

右邊“已選定”列表內的是當前被啓動且使用中的加密和哈希演算法； 如果使用者想要停止其中任何一種或多種的加密和哈希演算法， 可以使用 << ，將其移至左邊的“可選擇”列表內； 反之可以使用 >> ，將其再加回到右邊的“已選定”列表內。

在“已選定”列表右側的<上移>以及<下移>，用于調整各種加密和哈希演算法的協商優先等級； 在上端的優先等級較高，在下端的優先等級較低，使用者可以根據實際狀況自行調整。

## 3.5.2 會話管理

會話管理功能用于查看或强制結束當前連入的會話。一旦使用者遠端登入系統，幷成功獲得應用列表（即能看到 UU100 發布出來應用的圖示），會話即已建立起來了（該類會話也被稱爲 command tunnel）。

在系統主介面中（如圖 4）的“安全管理”之下，按下 會話管理 出現如圖 37 的視窗；視窗上會顯示當前所有的活動的 command tunnel(s)資訊，即所有連入 UU100 幷獲得應用列表的使用者的相關資訊。

可以在“現役的使用者列表”中選中會話記錄，將其强制斷開。




圖 37

## 3.6 系統參數管理

UU100 爲系統管理員提供以下系統管理功能：輸入和輸出系統配置，察看日志以及日志和報警等級的設定等。

### 3.6.1 匯入（/匯出）系統配置

在圖 4 的視窗中，選擇在“系統管理”之下的設定匯入，會顯示如圖 38 所示的視窗，將原來保存好的配置檔案輸入到系統中。

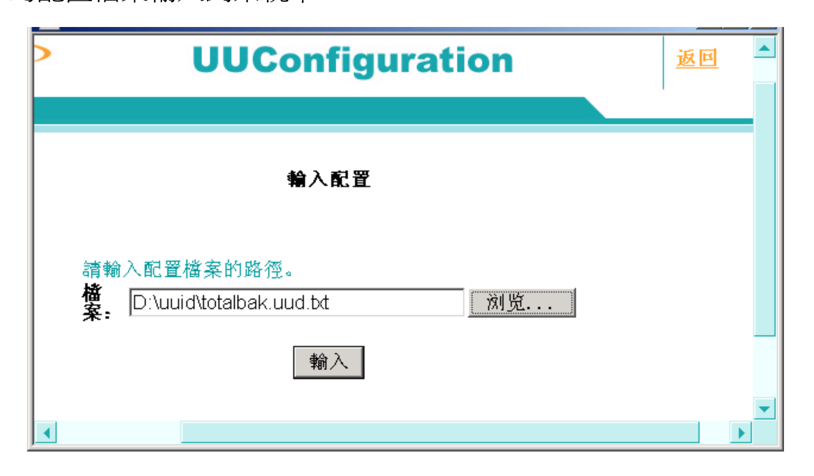



圖 38

按<瀏覽…>，選擇你原先輸出的系統配置檔案（參見本節“輸出配置”的內容），然後按下面的<輸入>，系統會提示下列資訊（圖 39），




圖 39

按 <確認>鍵，配置輸入完成。

在圖 4 的視窗中，選擇在“系統管理”下的輸出配置，會顯示如圖 40 所示的視窗，可以將配置檔案輸出到一個指定的檔案路徑，以複製檔案的形式保存起來。 您可以選擇輸出基本配置，輸出有關服務器資訊的配置，或是輸出整個系統配置。

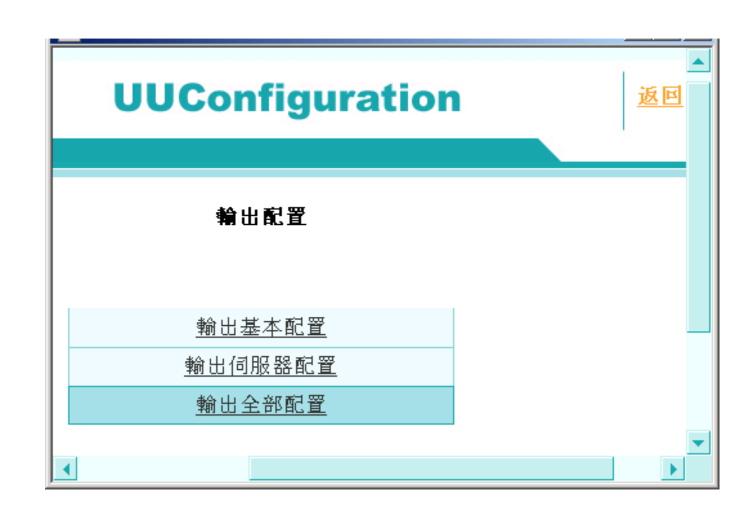



圖 40

初次進入這個介面，會顯示如圖 41 所示的安裝 ActiveX 的提示介面。 您必須按<是>，才能繼續完成輸出配置檔案。 (這是一個資料下載的控制項，不會對您的系統造成影響)




圖 41

## 3.6.2 管理許可證

許可證用來控制可以連接到 UU100 的最大同時上線人數。UU100 出廠時預設一個允許 10 個併發使用者的許可證。我們額外提供允許 25 個同時上線人數和 50 個同時上綫人數的許可證，如果需要可以向我們購買這兩種額外的許可證。

如果您已購買額外的許可證，可以通過以下步驟昇版許可證：

1. 點選"系統管理"下的管理許可證，進入下圖所示介面（圖 42）

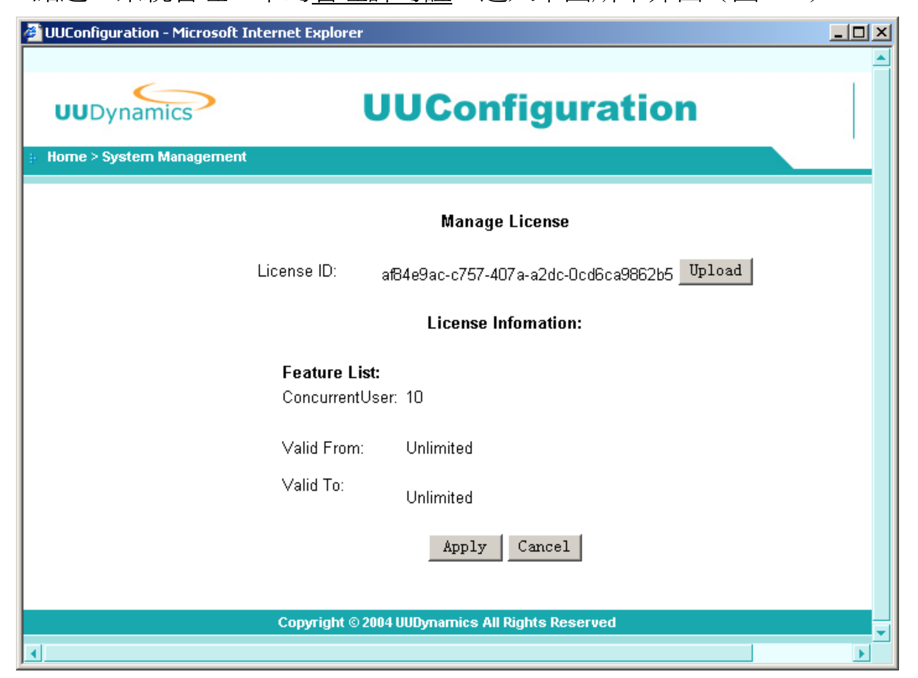



圖 42

2. 點選<上傳>，在圖 43 所示介面中點選<瀏覽>，選擇要替換的證書的完整路徑和檔案名稱，點選<確認>。

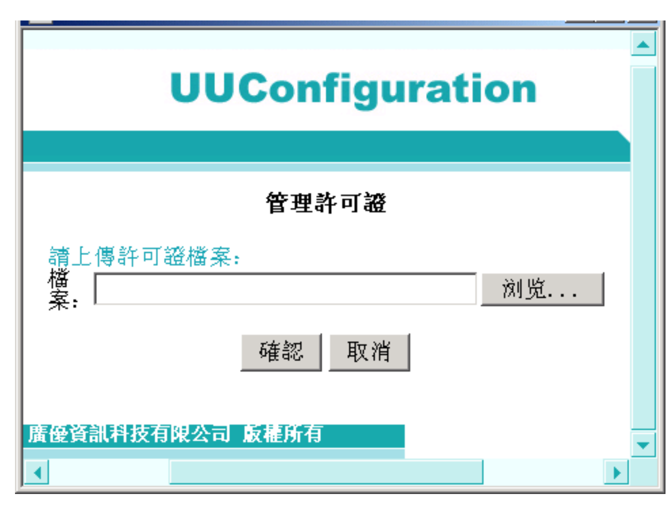



圖 43

3. 最後按<生效>，使當前的設定生效。

## 3.6.3 升版系統

您可以在本機或者通過遠端按照以下操作步驟升版系統版本：

1. 點選“系統管理”下的升版系統，進入圖 44 所示介面。

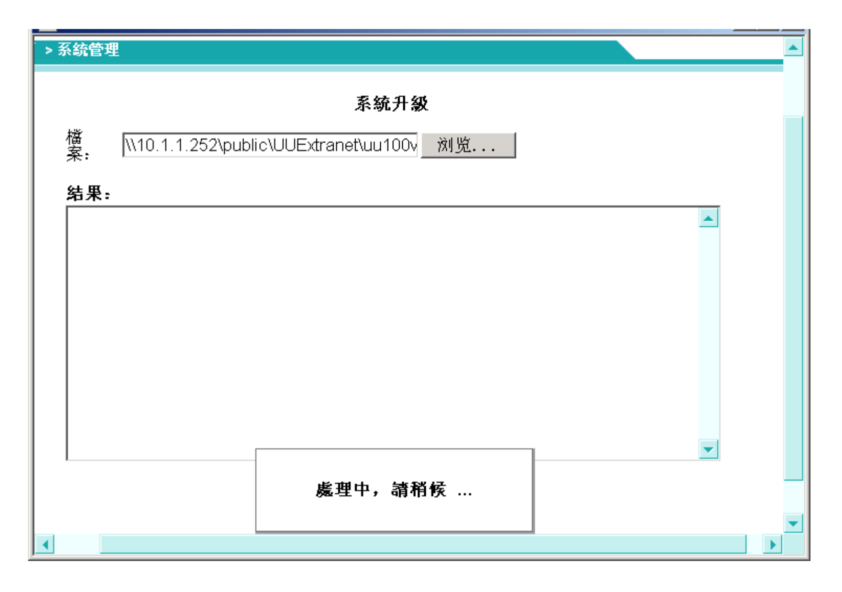



圖 44

2. 點選<瀏覽……>，選擇新版本的安裝程式的完整路徑和檔案名稱，點選<更新>。系統將自動完成版本升版。

## 3.6.4 故障檢修

我們爲您提供了三種常用的網路檢測工具：ping（檢測遠端主機或本地主機的連通性），traceroute（檢測從本地主機到遠端主機的路由），netstat（顯示網路連接、路由表和網路介面資訊）。您可以方便得在 UU100 的管理介面下使用這三種標準的檢測工具，監視和分析現有網路狀態，檢測網路連接性。(圖 45)

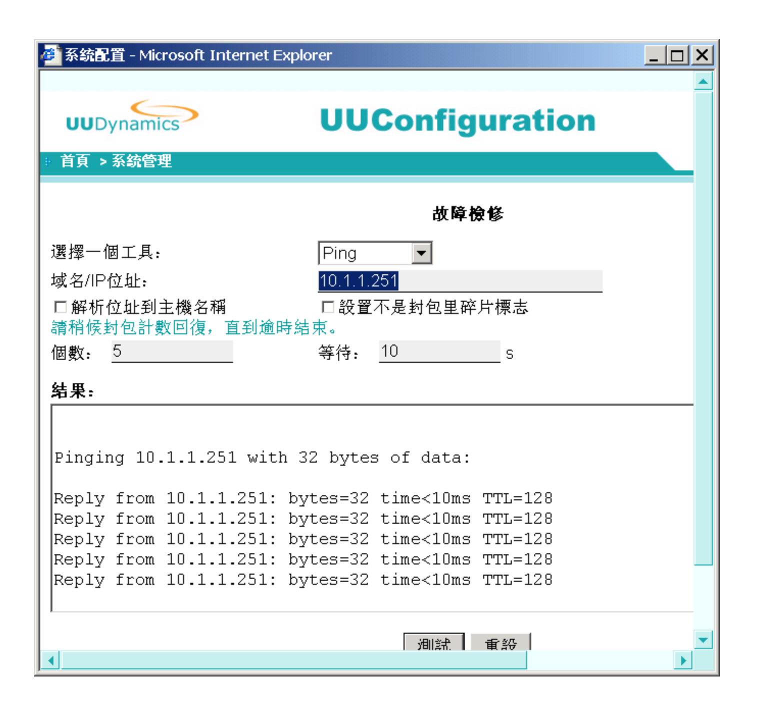



圖 45

## 3.6.5 顯示狀態

點選“系統管理”下的顯示狀態，可進入圖 46 所示介面察看系統當前的狀態，包括：UUID、運行狀態、路由表、當前版本等資訊。




圖 46

## 3.6.6 查看系統性能

在圖 4 的視窗中，選擇在“系統管理”之下的查看系統性能，可以查看連入 UU100 的連接數（Remote-desktops）或者使用者訂閱應用時 UU100 所使用的 data tunnels。

如圖 47 中所示，座標圖中的橫軸爲時間點，縱軸爲數量。紅色曲綫代表 Remote-desktops 的數量，綠色曲綫代表 Remote-data tunnels 的數量。如果近期 Remote-desktops 的數量持續逼近 Licence 數値，則說明該 UU100 的使用者數量已趨近最大值，此時應該考慮購買更多許可證以滿足日漸增長的需求。

點單擊<顯示>，靜態顯示選定時間段的統計資訊；

點單擊<現今>，動態顯示即時的統計資訊；

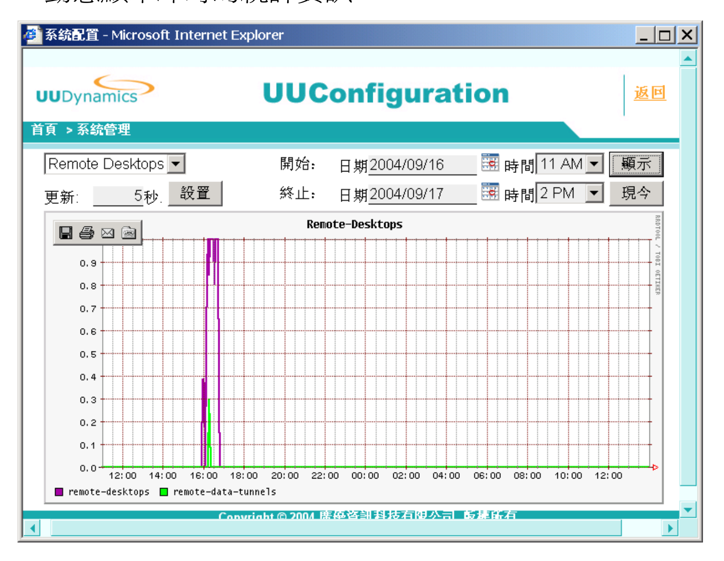



圖 47

## 3.6.7 日誌等級的設定

在圖 4 的視窗中，選擇在“系統管理”之下的日志控制，會顯示如圖 48 所示的視窗，系統管理員可以進行系統日志的設定。

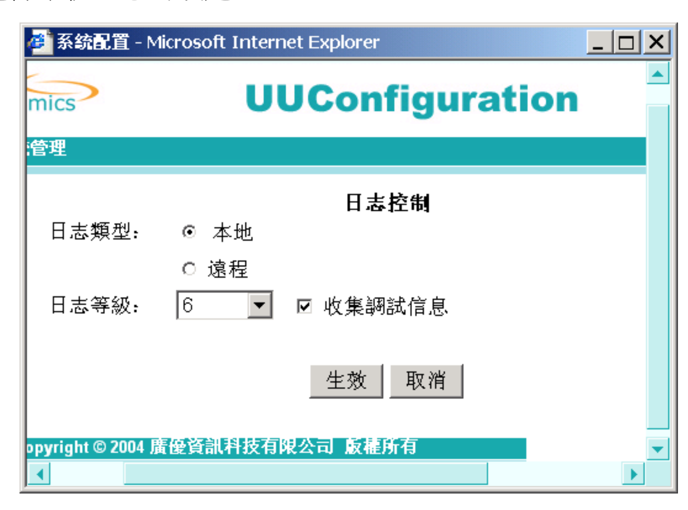



圖 48

其中，“日志類型”是指定日誌保存的地方。有“本地”和“遠端”兩種：“本地”是指將 UU100 的日志保存在本機上，而“遠端”可以將 UU100 的日志保存在遠端的 syslog 日誌伺服器上。

“日志等級”是指顯示和保存的日志詳細程度，總共有 0～6 級，等級越高，日誌越詳細，系統管理員可以根據實際需要來設定。以下是每一級別所代表的含義：

| 級別 | 含義 |
|---|---|
| 0 | No log（不作日志） |
| 1 | any condition that demand immediate attention（應該立即被糾正的情況） |
| 2 | critical conditions like hardware problems（嚴重情況） |
| 3 | any errors（一般性錯誤） |
| 4 | any warnings（警告） |
| 5 | conditions that may require attention（要注意的消息） |
| 6 | informational messages（資訊消息） |

勾選選中“收集調試資訊”核取方塊後，系統會將 debug 資訊寫入 Log 文件。

## 3.6.8 查看日誌

在圖 4 的視窗中，選擇在“系統管理”之下的顯示日志，會顯示如圖 49 所示的視窗。

系統管理員可以自行選擇查看特定時間段間的系統日志；系統管理員還可以自行選擇查看由 Level 0 到 Level 6 不同等級的日志情況，越高的等級表示日志的記錄越爲詳細。等級 0～6 的含義請參見“3.6.7 日誌等級的設定”

系統管理員可以選擇保存日志，以便日後使用。 在設定了要查看的日志時間範圍以及等級之後，按下<顯示>，可以顯示在設定條件下的全部日誌；

按<保存顯示日志>，則可以將螢幕上顯示的日誌保存到指定檔案路徑;

如果在設定日志等級時已勾選了“收集調試資訊”核取方塊，按下<全部保存>,則保存的 Log 文件中不僅包括螢幕上顯示的日志而且包含系統的 debug 資訊。

ⓘ 注意：

1. UU100 日誌中所紀錄的日期及時間，是根據 UU100 伺服器作業系統的設定日期及時間進行紀錄；您必需確定 Windows 伺服器的日期及時間設定正確，才能獲得正確的日誌紀錄。
2. 日誌資訊[ ]符號外部的內容，爲出錯提示，供使用者參考。[]內部的內容，爲系統內部資訊，供開放人員跟踪。使用者可以不予理會，如有需要，亦可將其告知我公司技術支援人員。

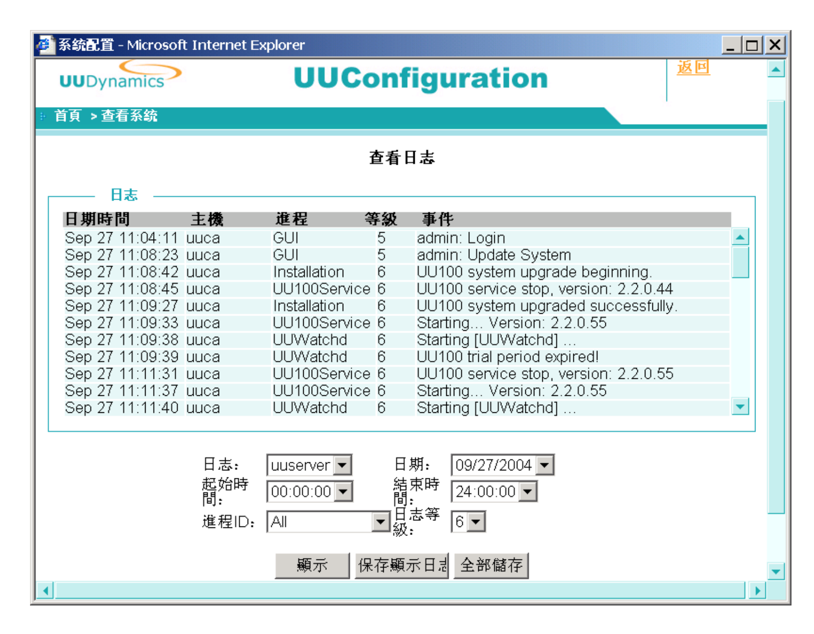



圖 49

## 3.6.9 告警等級的設定

在圖 4 的視窗中，選擇在“系統管理”之下的告警設置，會顯示如圖 50 所示的視窗。

“告警等級”是指發出警告資訊的日志級別，例如，設定告警等級爲 5，則表示如果有 5 級及以下的日志產生的話，就以警告的形式通知系統管理員。

系統管理員可以設定報警等級，幷發往指定的電子郵件地址。

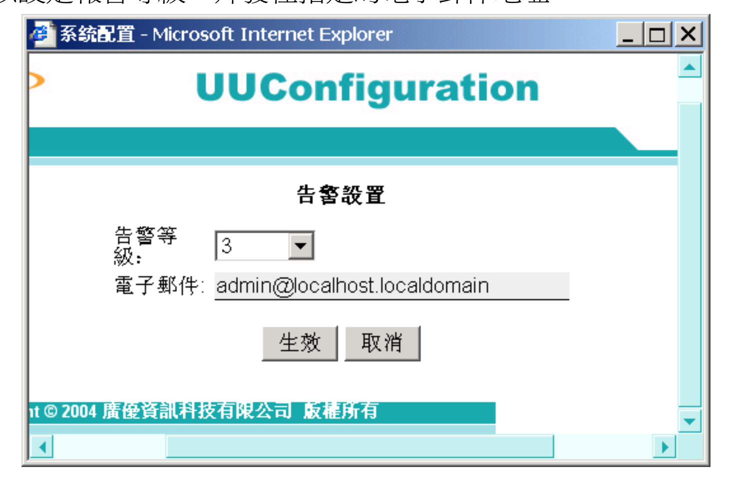



圖 50

## 3.6.10 系統時間及 LOGO 設定

在圖 4 的視窗中，選擇在“系統管理”之下的系統設定,您可以修改 UU100 的系統時間（圖 51），或是修改顯示在左上角的 LOGO 文件（圖 52），您可以使用您公司的 LOGO 替換它，但必須是 gif 文件格式，Size 小於 5KB。

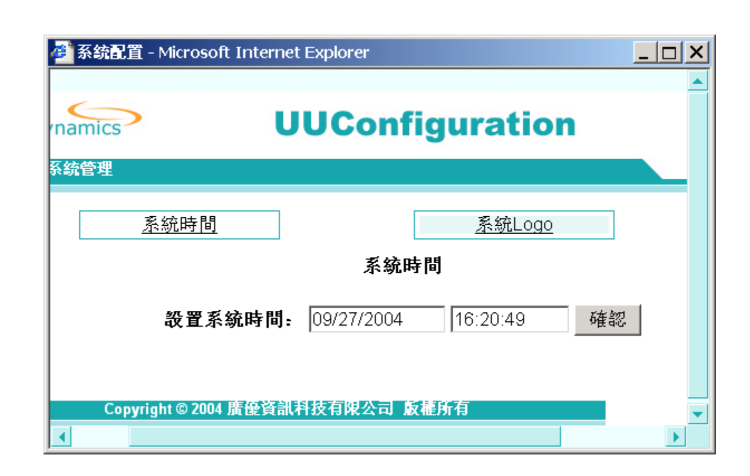



圖 51

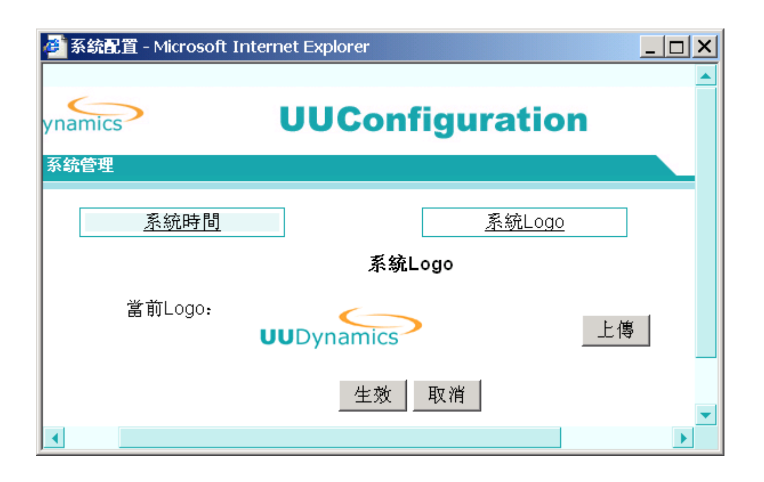



圖 52

# 3.7 進階

## 3.7.1 選擇網路模式

如圖 53 所示，UU100 只支援“單模式”，這種模式允許 UU100 被安裝于內部網路中的任意位置的一種模式，其特點是無需改變原網路中任何設備的配置，隨意、隨時插到企業任何可上廣域網的網路上就可工作，非常簡單、便捷。

📖 說明：

選擇“預設出廠（重設）”模式，可以將已有的配置清除掉，并將 UU100 恢復到出廠設定。

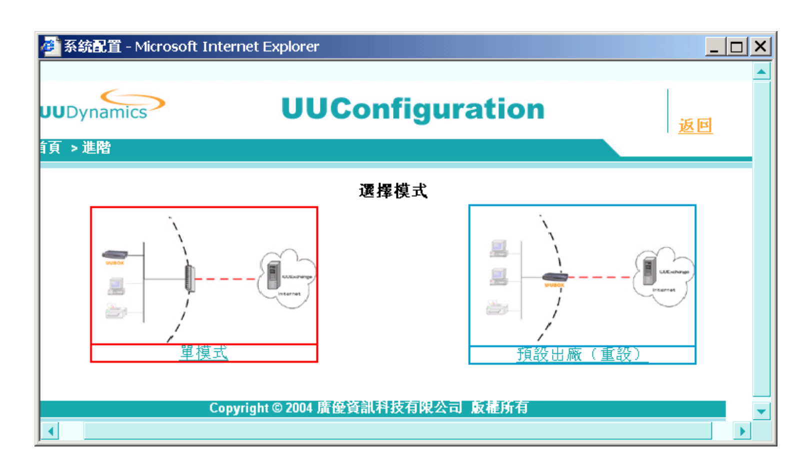

系統配置 - Microsoft Internet Explorer
UUDynamics
UUConfiguration
返回
首頁 > 進階
選擇模式
單模式
預設出廠（重設）
Copyright © 2004 廣優資訊科技有限公司 版權所有

圖 53

# 第4章 發佈應用

每個 UU100 能發佈不超過 100 個應用。每個應用允許設定總數不超過 100 個的接入規定，其中包括：需要接入的機器、需要接入的使用者或者需要接入的埠。

在發布應用程式設定視窗介面中（如圖 54），按下<增加>；您會看到一些預設的應用程式選擇專案（如圖 55），它們計有：Internet Explorer，CVS, Outlook, Telnet, Ftp, Netmeeting, pcAnywhere 等等常用的應用程式； 此外還有一個“Custom”選擇專案，當您要發佈的應用程式不存在於預設的應用程式選擇專案之中，您便可以使用“Custom”來設定該應用程式的發佈。 另外，由 UUDynamics 所提供的遠端檔案瀏覽程式“UUDynamics File Browser”和“UUDynamics File Browser Express”也在選擇專案中。

有關“UUDynamics File Browser”和“UUDynamics File Browser Express”的相關配置及使用方法，詳見本使用手冊的附錄部分。”

有關 ***i*STAR™**支援的客戶/伺服器應用及其所受限制，請參考本使用手冊的附錄部分”

## 4.1 增加應用程式

以發佈“Internet Explorer”爲例：

1. 如圖 54，爲保證遠端使用者存取應用時建立的 SSL 連接的安全，您可以設定允許會話持續的最長時長和允許會話空閑的最長時長。超過設定的時長，系統會自動斷開這次連接。
2. 如果勾選“允許同一使用者多次訪問”， 則同一使用者再次（或使用同樣的使用者名稱從其他機器）獲取應用列表時，不影響之前以該使用者名稱獲取應用列表的其他會話。
   反之，如果不勾選該選項，則登入時會强行中止之前的所有以該使用者名稱獲取應用列表的會話。
3. 按下<增加>，進入圖 55 的視窗；
4. 選擇“Internet Explorer” ，按<確認>，進入圖 56 的視窗；
5. 在“名稱”欄中，您可以輸入您爲這個 Internet Explorer 應用所取的名稱；
6. 勾選“啓用加密”會啓動系統設定的加密演算法；
7. 勾選“啓用 Hash”會啓動系統設定的 Hash 演算法；
8. 勾選“啓用壓縮”會啓動系統設定的壓縮演算法；
9. 如果 Internet Explorer 應用所對應的伺服器和 UU100 是同一台伺服器，則可以勾選“本端伺服器站點” ，出現如圖 57 所示的介面；此時不需要爲 Internet Explorer 應用特別填寫 IP 位址；
   如果 Internet Explorer 應用所對應的伺服器和 UU100 不是同一台伺服器，就不能勾選“本端伺服器站點” ，而必需在“IP 位址：”欄中輸入該應用所對應的伺服器 IP 位址；如果您的 Internet Explorer 應用所對應的伺服器具備 DNS 名稱，也可以在“功能變數名稱：” 欄中輸入這個 Internet Explorer 應用所對應的伺服器 DNS 名稱；而按“<-DNS 查找->”鍵可以自動將伺服器的 DNS 名稱轉換爲 IP 位址，或是將伺服器的 IP 位址轉換爲 DNS 名稱。
10. 勾選“啓動公共站點訪問”表示遠端使用者不僅可以通過 IE 訪問上述指定 IP 位址的 Web 應用，而且還可以訪問該地址以外的站點頁面。這對于使用了外部

鏈結的 Web 應用尤其適用，如果沒有勾選這個選項，則所有超鏈結都無法使用。

11. 在“該應用在使用者端機器上的默認路徑：”欄中所顯示的，是指遠端使用者在使用這個應用程式時（此處是 Internet Explorer），遠端使用者電腦中的客戶端應用軟體路徑的預設位置； 因爲本例中的應用爲 Internet Explorer，所以客戶端軟體爲 IE 瀏覽器，預設路徑爲“%ProgramFiles%\Internet Explorer\iexplorer.exe”；
12. 在“使用者端機器運行該應用時所需的參數：”欄中所顯示的，是指遠端使用者在使用這個應用程式時，遠端使用者電腦中的客戶端應用軟體預設的運行參數；在本例中運行的是 Internet Explorer，參數的設定即是您允許遠端使用者訪問的 URL。
13. 點選<規定…>，進入圖 58 所示的視窗。輸入您爲這個策略所取的名稱；目前 UU100 僅能提供驗證證書這一發佈策略，更多策略方案將陸續提供。
14. 點選<使用者…>，根據需要增加使用者（/組/角色）。進入圖 59 所示的視窗；將使用者所屬的安全域從“可選擇”列表框中移至“已選定”列表框。如果選擇的是包含有角色角色資訊的 Radius 或 PKI 類型的安全域，會顯示圖 60 所示的操作介面。
15. 設定該應用的訂閱策略，系統預設的是“拒絕”，意即所有的使用者都不能訂閱該應用。
16. 在“使用者列表”中指定排除在訂閱策略之外方式。在其下的“使用者列表”列表中勾選使用者(/組/角色)，並按<增加>將其加入下方的“除了以下列出的”目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者（/組/角色）。

    通過這一步驟結合設定訂閱策略步驟相結合，管理員可以靈活的設定應用的使用範圍，即：僅允許某一些使用者訂閱所發佈應用，或者允許除某一些使用者外的所有使用者訂閱。
17. 按下<返回>返回圖 56 的視窗；
18. 按下<埠範圍>，進入圖 61 的視窗；
19. 本例爲 Internet Explorer 應用，因此系統預設的埠範圍爲 80。 您可以按<增加>增加新的埠範圍（如圖 62），使用<編輯>鍵對既有的埠範圍進行編輯，或使用<移除>移除既有的埠範圍；
20. 按下<返回>返回圖 56 的視窗；
21. 按下<確認>完成對發佈 Internet Explorer 的設定

對於其他預設應用程式選擇專案內已有的應用程式發佈方法，都和以上發佈 Internet Explorer 應用的程式的方法類似，您可以參照以上方法發布其他各種應用程式。

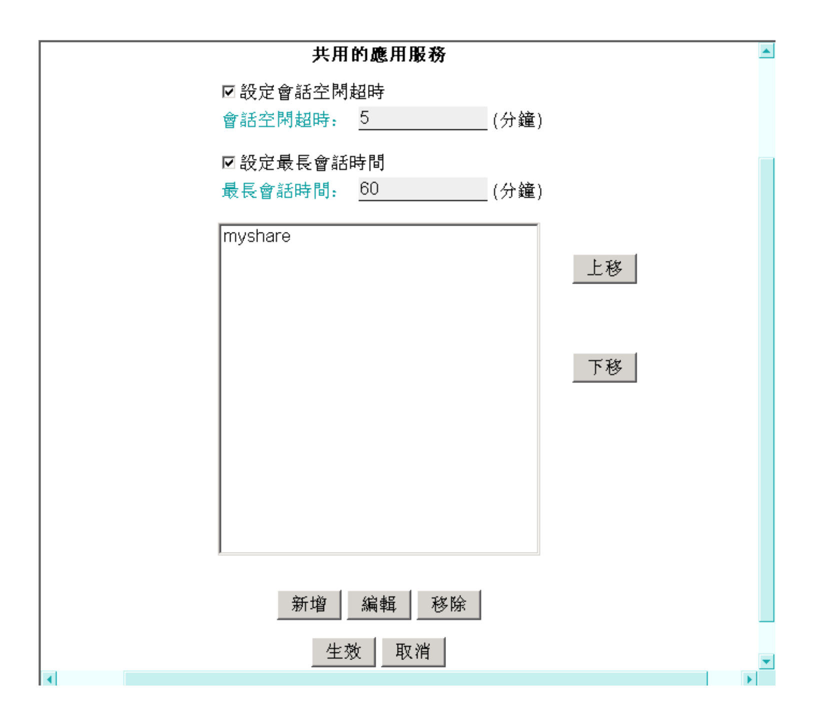

共用的應用服務
設定會話空閑超時
會話空閑超時： 5 (分鐘)
設定最長會話時間
最長會話時間： 60 (分鐘)
myshare
上移
下移
新增
編輯
移除
生效
取消

圖 54

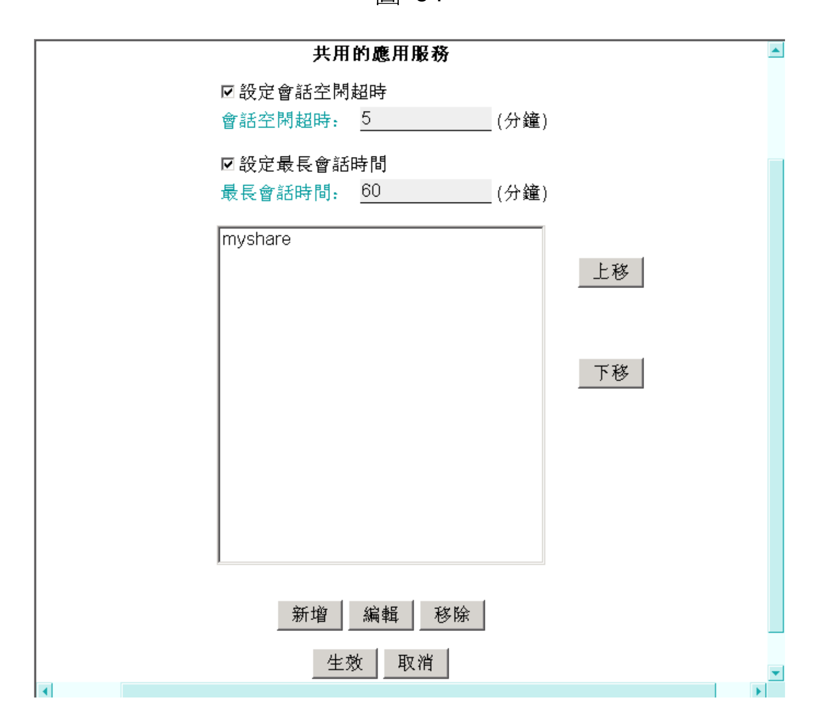

共用的應用服務
設定會話空閑超時
會話空閑超時： 5 (分鐘)
設定最長會話時間
最長會話時間： 60 (分鐘)
myshare
上移
下移
新增
編輯
移除
生效
取消

圖 55

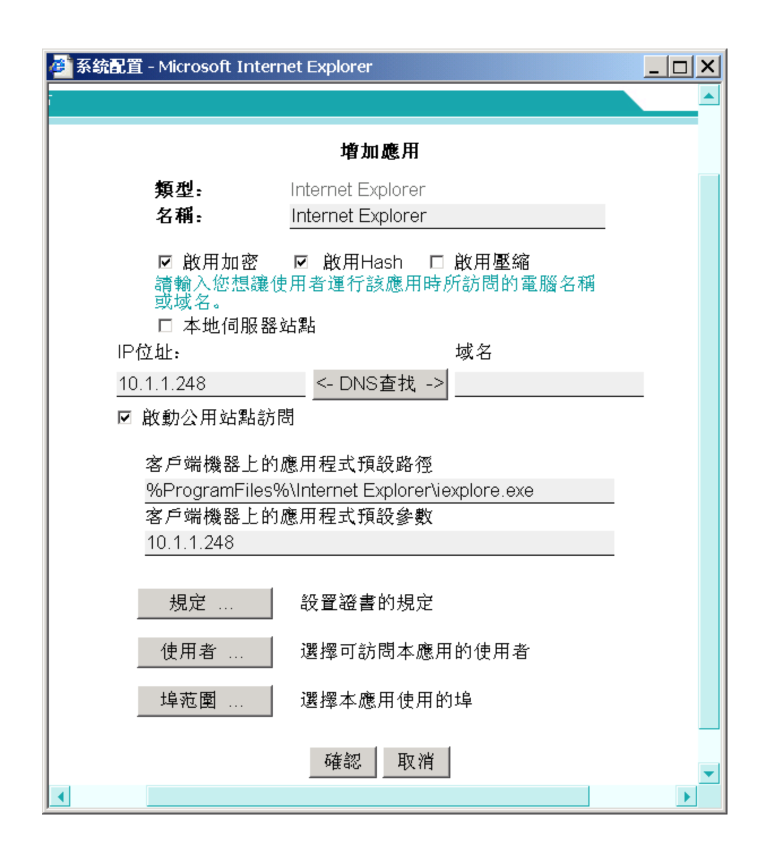



圖 56

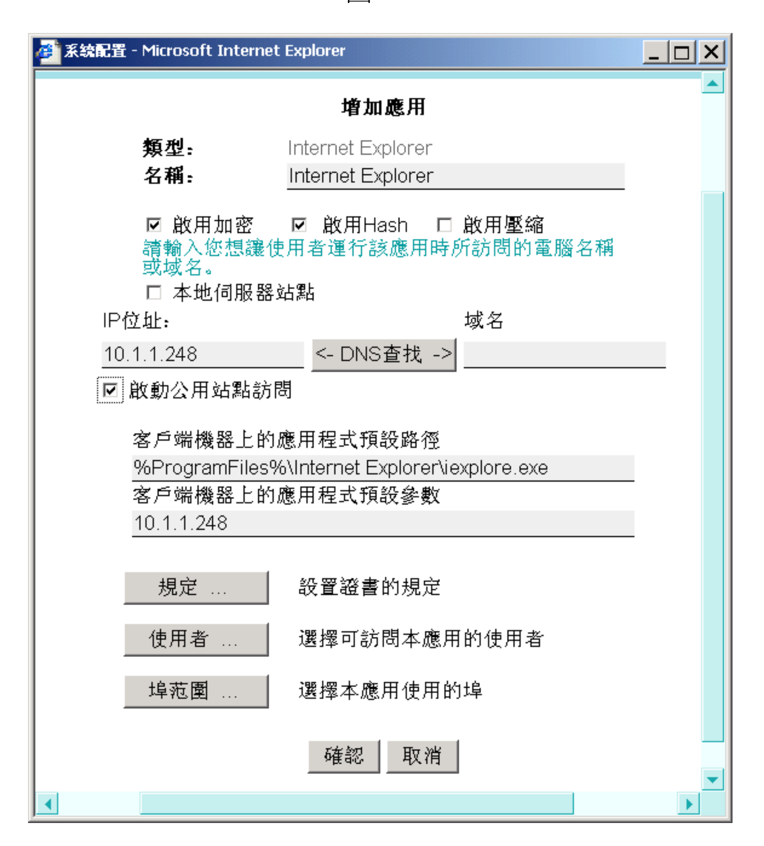



圖 57

| 參數/控鍵 | 含義 | 備註 |
|---|---|---|

| 名稱 | 指共用應用程式的名稱 | |
|---|---|---|
| 啓用加密 | 表示該共用的應用程式通過 Encrypt 演算法 | Encrypt 演算法:是指對傳輸資料進行加密的策略，通常標準的演算法有：AES、3DES、DES 等。***i*STAR™**系列產品采用的就是以上這三種演算法，幷可以任意選擇。NULL 表示不加密，用明文傳輸。 |
| 啓用 Hash | | Hash 演算法:表示該共用的應用程式通過演算法。Hash 演算法是指把資訊進行混雜，使得它不可能恢復原狀的策略。這種形式的加密將產生一個 HASH 值，這個值帶有某種資訊，幷且具有一個長度固定的表示形式。***i*STAR™**系列產品采用的是 MD5、SHA1 這兩種 hash 演算法，可以任意選擇。 |
| 啓用壓縮 | 系統將對資料包進行壓縮 | |
| IP 位址 | 指該應用所在的伺服器的 IP 地址 | |
| DNS 查找 | 表示可將 IP Address 轉換成 DNS 名稱 | |
| 該應用在用戶端機器上的默認路徑 | 指共用的應用程式指在使用者端電腦上的預設路徑。 | 雖然系統裏發布的是指定伺服器上的相關應用，但是在使用者端電腦上一定要安裝有該應用。 |
| 用戶端機器運行該應用時所需的參數 | 指共用的應用程式在使用者端上運行的參數。 | |
| 規定… | 進入設定允許存取該共用應用程式的策略介面 | |
| 使用者… | 進入設定允許（/禁止)存取該共用應用程式的使用者介面 | |
| 埠範圍… | 進入設定開放的埠介面 | 如果增加的是“Custom – Roaming application”應用，則不需要指定埠範圍。 |


系統配置 - Microsoft Internet Explorer
Dynamics
UUConfiguration
>認證
增加 / 編輯發布規定
名稱:
Internet Explorer
經由證書 / PKI認證
可供選擇的根CA:
已選擇的根CA:
/C=US/O=RSA Data Se
/C=CN/ST=SH/L=SH/O
/C=US/ST=CA/L=Cupe
>>
<<
證書限制:
確認
取消

圖 58


系統配置 - Microsoft Internet Explorer
可供選擇
已選擇
My AD/LDAP Realn
MyRadius
LocalRealm
> >
< <
設置使用者和群組的權限
預設訪問規定 拒絕 允許
使用者列表: 使用者 群組
使用者列表
名稱
類型
admin 使用者
kathy 使用者
qin 使用者
增加
全部選擇
取消選擇
除了下列的
群組/使用者名稱
類型
qin 使用者

圖 59


系統配置 - Microsoft Internet Explorer
可供選擇
My AD/LDAP Realn
已選擇
LocalRealm
MyRadius
> >
< <
設置使用者和群組的權限
預設訪問規定 拒絕 允許
使用者列表: 使用者 角色
使用者列表
名稱
類型
admin
角色
HR
角色
增加
全部選擇
取消選擇
除了下列的
群組/使用者名稱
類型
HR
角色

圖 60

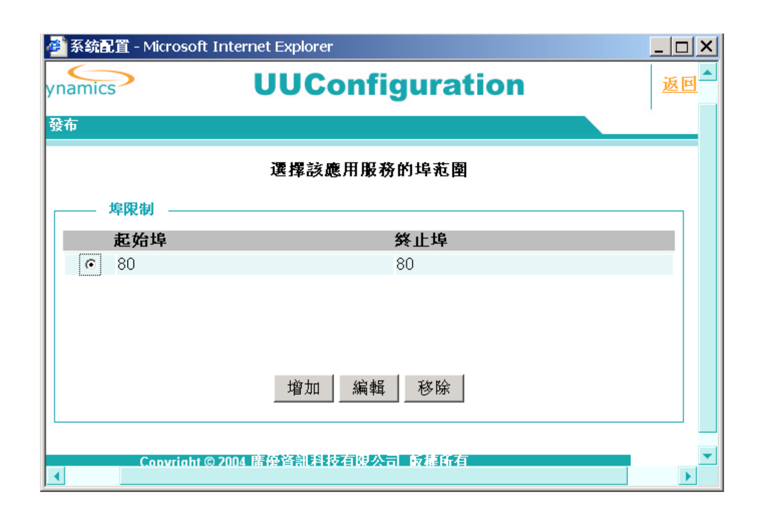

系統配置 - Microsoft Internet Explorer
UUConfiguration
返回
發布
選擇該應用服務的埠范圍
埠限制
起始埠
終止埠
80
80
增加
編輯
移除

圖 61

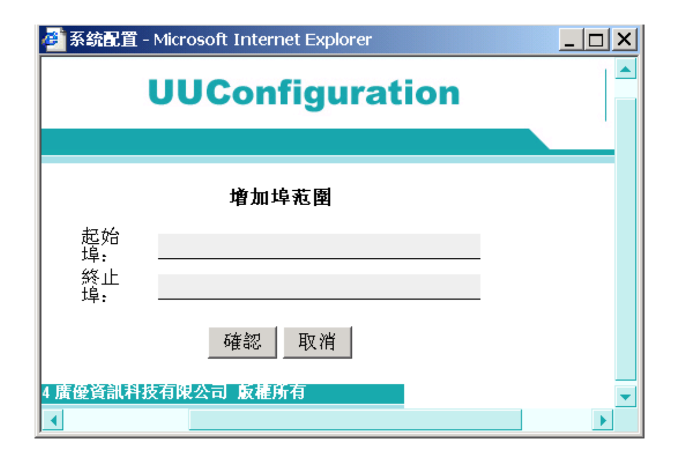

系統配置 - Microsoft Internet Explorer
UUConfiguration
增加埠范圍
起始埠:
終止埠:
確認
取消

圖 62

## 4.2 定制新的應用程式

您可以增加“Custom”類應用以定制自己的服務。目前 UU100 中提供三種“Custom”應用：

Custom – Multi-station application：遠端使用者通過 UU100 存取多台機器中任一台的指定埠。如此，使用者便可存取任一台機器的相同服務。例如，存取多個 Web 伺服器的 Internet Explorer，就是這樣的應用。

Custom – Roaming application：遠端使用者通過 UU100 存取多台機器中的任一台的某一個埠。這時，管理員需要單獨指定每一台被存取的機器埠號。通常情況下，使用者通過該 UU100 可以存取任一台機器的任一服務。例如，需要存取多個伺服器的 ERP 軟體，需要同時訪問資料庫伺服器、應用伺服器等，這時便可使用這一應用。

Custom – Network drive based C/S：該應用支援遠端 Client 端用戶象使用網路盤符一樣存取由 UU100 發布的共用資源（Client 端運行的應用程式已將此共用資源對應爲指定的網路映射盤）。例如：現有一個 MIS 系統，已將 Database 的完整路徑對應到網路映射盤“N：”，并且管理員在 UU100 中將該 Database 發佈。這樣，多個 Client 端使用者便可同時對該 Database 進行操作。

### 例一：以發佈“Custom – Multi-station application”爲例：

1. 如圖 54，爲保證遠端使用者存取應用時建立的 SSL 連接的安全，您可以設定允許會話持續的最長時長和允許會話空閑的最長時長。超過設定的時長，系統會自動斷開這次連接。
2. 按下<增加>，進入圖 55 的視窗；
3. 選擇“Custom – Multi-station application”，按<確認>，進入圖 63 的視窗；
4. 在“名稱：”欄中，您可以輸入您爲這個 Custom 應用所取的名稱；
5. 勾選“啓用加密”會啓動系統設定的加密演算法；（詳見本手冊“4.1 增加應用程式”的表格中的說明）
6. 勾選“啓用 Hash”會啓動系統設定的 Hash 演算法；（詳見本手冊“4.1 增加應用程式”的表格中的說明）
7. 勾選“啓用壓縮”會啓動系統設定的壓縮演算法；
8. 在“該應用在用戶端機器上的默認路徑”欄中所顯示的，是指遠端使用者在使用這個應用程式時，遠端使用者電腦中的客戶端應用軟體路徑的預設位置；
9. 在“用戶端機器運行該應用時所需的參數”欄中所顯示的，是指遠端使用者在使用這個應用程式時，遠端使用者電腦中的客戶端應用軟體預設的運行參數；
10. 點選<規定…>，進入圖 58 所示的視窗。輸入您爲這個策略所取的名稱；
    目前 UU100 僅能提供驗證證書這一發佈策略，更多策略方案將陸續提供。
11. 點選<使用者…>，根據需要增加使用者（/組/角色）。進入圖 59 所示的視窗；將使用者所屬的安全域從 Available 列表框中移至”已選定”列表框。如果選擇的是包含有角色角色資訊的 Radius 或 PKI 類型的安全域，會顯示圖 60 所示的操作介面。
12. 設定該應用的訂閱策略，系統預設的是“拒絕”，意即所有的使用者都不能訂閱該應用。
13. 在“使用者列表”中指定排除在訂閱策略之外方式。在其下的“使用者列表”列表中勾選使用者（/組/角色），並按<增加>將其加入下方的“已選定的使用者”

目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者（/組/角色）。

通過這一步驟結合設定訂閱策略步驟相結合，管理員可以靈活的設定應用的使用範圍，即：僅允許某一些使用者訂閱所發佈應用，或者允許除某一些使用者外的所有使用者訂閱。

14. 按下<返回>返回圖 63 的視窗；
15. 按下<電腦……>，進入圖 64 的視窗，選擇這個 Custom 應用所對應的伺服器（組）；可以選擇“所有電腦”或“無電腦”，然後按下<增加>, 進入圖 65 的視窗；
16. 根據 Custom 應用所對應的伺服器（組）的實際情況，勾選“單個電腦”，“電腦組”或者“功能變數名稱”；如果是“單個電腦”，可以填寫伺服器的 IP 位址或是 DNS 名稱；如果是“電腦組” 可以填寫伺服器組的網路位址和子網路遮罩，如圖 66；如果是““功能變數名稱”可以填寫伺服器（組）DNS 名稱，如圖 67；按下<確認>進行確認；鍵返回圖 65 的視窗，您將會在視窗中的“除了以下列出的”內看見被新加入的伺服器（組）的資訊； 按<返回>返回圖 63 的視窗；
17. 按下<埠範圍……>，進入圖 69 的視窗；
    如果增加的是“Custom – Roaming application”應用，則不需要指定埠範圍。
18. 按<增加>增加新的埠範圍，填寫起始埠和終止埠；
19. 按下<返回>返回圖 63 的視窗；
20. 按下<確認>完成對發佈 Custom 應用的設定，並點選<生效>使設定生效。




圖 63


系統配置 - Microsoft Internet Explorer
ynamics
UUConfiguration
返回
發布
選擇運行該應用服務的電腦
在'無電腦'情況下，按'增加'按鈕，可以加入在運行應用時，允許使用者訪問的電腦。
在'所有的電腦'情況下，按'增加'按鈕，可以加入在運行應用時，禁止使用者訪問的電腦。
當前客戶可以訪問：
所有的電腦 無電腦
除了下列的
類型 IP位址（掩碼）/域名
ipaddress 10.1.1.224
增加 編輯 移除
Copyright © 2004 廣僑資訊科技有限公司 版權所有

圖 64


系統配置 - Microsoft Internet Explorer
mics
UUConfiguration
允許訪問
單機（電腦） 群組電腦 域名
輸入使用者在運行該應用時可以訪問的電腦名稱或域名.
IP位址：
確認 取消
Copyright © 2004 廣僑資訊科技有限公司 版權所有

圖 65


系統配置 - Microsoft Internet Explorer
UUConfiguration
> 發布
允許訪問
單機（電腦） 群組電腦 域名
輸入使用者在運行該應用時可以訪問的電腦名稱或域名.
網路位址:
10.1.1.220
子網掩碼:
255.255.255.0
確認 取消

圖 66


系統配置 - Microsoft Internet Explorer
UUConfiguration
允許訪問
單機（電腦） 群組電腦 域名
輸入使用者在運行該應用時可以訪問的電腦名稱或域名.
域名:
uud
確認 取消
Copyright © 2004 廣優資訊科技有限公司 版權所有

圖 67

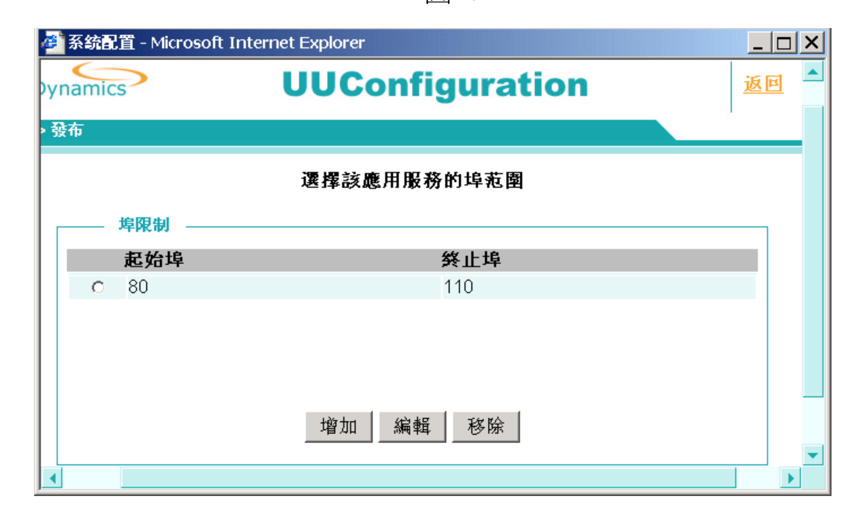

系統配置 - Microsoft Internet Explorer
UUConfiguration
返回
> 發布
選擇該應用服務的埠范圍
埠限制
起始埠
終止埠
80
110
增加 編輯 移除

圖 68

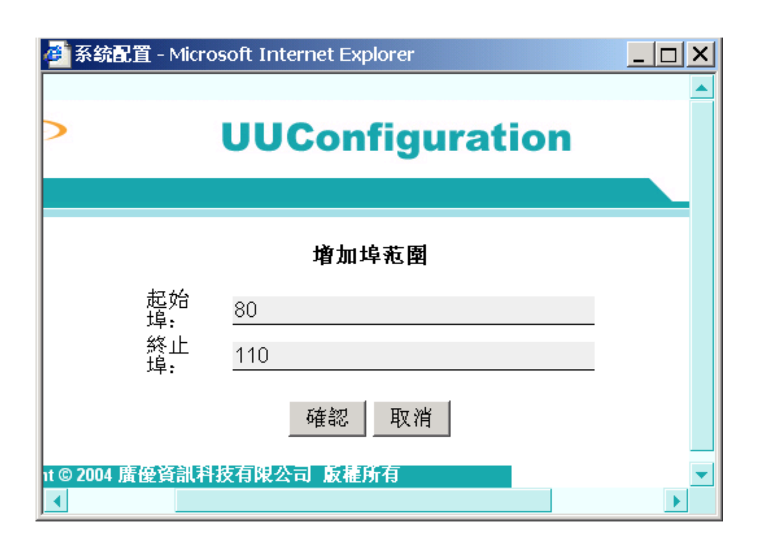



圖 69

例二：以發佈“**Custom – Network drive based C/S**”爲例：

1. 如圖 54，爲保證遠端使用者存取應用時建立的 SSL 連接的安全，您可以設定允許會話持續的最長時長和允許會話空閑的最長時長。超過設定的時長，系統會自動斷開這次連接。
2. 按下<增加>，進入圖 55 的視窗；
3. 選擇“Custom – Network drive based C/S”，按<確認>，進入圖 70 的視窗；

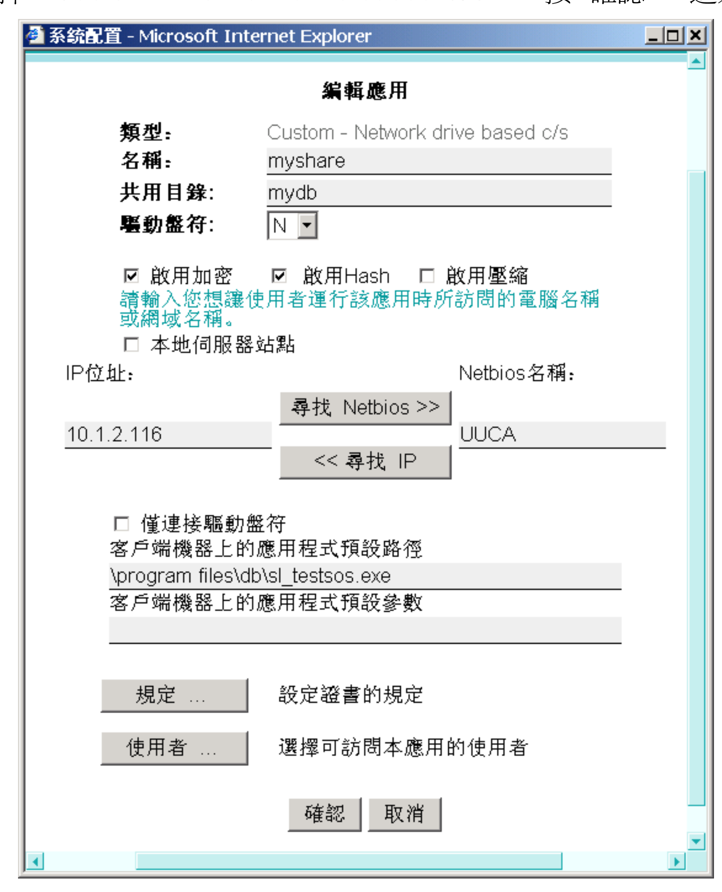



圖 70

4. 在“名稱:”欄中，輸入您爲這個應用所取的名稱；
5. 在“共用目錄：”欄中，輸入您要作對應的 Folder 名稱，並請確保輸入正確；
6. 勾選“啓用加密”會啓動系統設定的加密演算法；(詳見本手冊“4.1 增加應用程式”的表格中的說明)
7. 勾選“啓用 Hash”會啓動系統設定的 Hash 演算法;(詳見本手冊 4.1 增加應用程式的表格中的說明)
8. 勾選“啓用壓縮”會啓動系統設定的壓縮演算法；
9. 如果該應用要對應的盤符在本機，則可以勾選“本端伺服器站點”，此時不需要爲 Internet Explorer 應用特別填寫 IP 位址；如果該應用要對應的盤符不在本機，就不能勾選“本端伺服器站點”，而必需在“IP 位址：”欄中輸入該盤符所在的伺服器 IP 位址；或在“Netbios 名稱” 欄中輸入該盤符所在的伺服器的 Netbios 名稱。
   按 Lookup Netbios >> 鍵可以將伺服器的 IP 位址自動轉換爲 Netbios 名稱;
   按 << Lookup IP 可以將伺服器的 Netbios 名稱自動轉換爲 IP 位址。
10. 如果僅將某一個目錄下的內容對應成爲用戶端的虛擬碟符而不需要發布相應程式，則可以選擇“僅連接驅動盤符”。否則不要選中該項。
11. 在“該應用在用戶端機器上的默認路徑”欄中所顯示的，是指遠端使用者在使用這個應用時，遠端使用者電腦中的客戶端應用軟體路徑的預設位置；
12. 在“用戶端機器運行該應用時所需的參數”欄中所顯示的，是指遠端使用者在使用這個應用時，遠端使用者電腦中的客戶端應用軟體預設的運行參數。
13. 點選<規定…>，進入圖 58 所示的視窗。輸入您爲這個策略所取的名稱；
   目前 UU100 僅能提供驗證證書這一發佈策略，更多策略方案將陸續提供。
14. 點選<使用者…>，根據需要增加使用者（/組/角色)。進入圖 59 所示的視窗；將使用者所屬的安全域從“可選擇”列表框中移至“已選定”列表框。如果選擇的是包含有角色角色資訊的 Radius 或 PKI 類型的安全域，會顯示圖 60 所示的操作介面。
15. 設定該應用的訂閱策略，系統預設的是“拒絕”，意即所有的使用者都不能訂閱該應用。
16. 在“使用者列表”中指定排除在訂閱策略之外方式。在其下的“使用者列表”列表中勾選使用者(/組/角色),並按<增加>將其加入下方的“已選定的使用者”目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者（/組/角色)。
   通過這一步驟結合設定訂閱策略步驟相結合，管理員可以靈活的設定應用的使用範圍，即：僅允許某一些使用者訂閱所發佈應用，或者允許除某一些使用者外的所有使用者訂閱。
17. 按下<返回>返回圖 70 的視窗；
18. 按下<確認>完成對發佈 Network drive based C/S 的設定，並點選<生效>使設定生效。

對于其他預設應用程式選擇專案內已有的應用程式發布方法,都和以上發布的兩種應用的方法類似，您可以參照以上方法發布其他各種應用程式。

## 4.3 編輯（更改）已發布的應用程式

在圖 4 的視窗中，選擇在“發布”之下的發布應用，會顯示如圖 54 所示的視窗。

“共用的應用服務”列表中，列出了已發布的應用，選擇其中的某一項，點選<編輯>，可以更改該項應用的配置。（請參考圖 56）完成編輯後，請務必記得點選<生效>，使所做的更改生效。

更改已發布應用的任一配置，僅會對此後連入 UU100 的 Session 生效，即不會影響更改之前已經連入 UU100 的 Session。

例如，某一使用者現正通過 UU100，使用 IE 服務。此時如果將該使用者從已發布的 IE 應用中移除，并不會影響該使用者的任何操作。但是，一旦該使用者登出，本次 Session 結束，則將無法重新建立另一個新的 Session，再次登入該台 UU100。

# 第5章 故障檢測和排除

（1） 完成基礎設定後，結果連接或註冊 UUExchange 失敗，爲什麼？

a) 網路設定不正確，請檢查路由。使用 ping 工具檢查是否能夠 ping 通 UUExchange。

b) 運行 Telnet uuswitch 443 檢查是否能夠連接到 UUSwitch/UUExchange。檢查網路設定是否正確，UUExchange/UUSwitch 是否已經啓動。

c) 如果連接成功，註冊不成功，檢查 UUID File 是否正確；

d) 如果證書正確，應確保 UUExchange/UUSwitch 上確有此 UUID，沒有被 Disable 或刪除,也沒有被 Renew, UUID 也沒有過期。

（2） 發布應用程式、發布子網或遠端管理時，遠端使用者無法訂閱相關內容，爲什麼？

***i*STAR™**處理的連接和加密針對的是通信雙方的應用通道，而非雙方主機間的整個通道。因此，首先應確保所有應用在區域網路裏能够正常使用，以排除 Internet 連接等外部因素引起的故障。有些應用的配置複雜，部署時牽涉多項事件，稍有差錯便無法運行，如 MS Outlook 等便是較典型的例子。

此外還需檢查這些應用是否屬於 ***i*STAR™**支援的客戶/伺服器應用（請參閱附錄）。

如以上要求均已滿足，而在遠端的使用者仍無法訂閱，則請逐一排除以下可能原因：

a) 未選擇正確的認證方式：

如果使用伺服器認證，請先確保此域存在，且可訪問。

如果切換了認證方式，所有應用中的使用者設定將刪除。此時，應該爲每個應用程式重新配置使用者。如果安全域 LocalUsers 或其他認證伺服器中使用者有改變，也應檢查應用中的使用者設定是否正確。

b) DNS 服務未能正確解析該 DNS 名稱：

如果在電腦設定中，使用 DNS 名稱配置，請應確保 Publisher 的 DNS 能解析該 DNS 名稱。如果配置的是域，應確保能够反向解析。否則，如果設定爲“除了配置的機器，其他的機器都不能訪問”時，將會發生錯誤。

（3） 訂閱不到已發佈的應用程式，問題在哪？

a) 訂閱者和發佈者是否都已連接上同一個 UUExchange，並且均註冊成功。

b) 使用者名稱，密碼，域是否填寫正確。

（4） 選擇網路模式時應注意哪些問題？

根據 UUExchange 所在網路中的實際情況，選擇正確的模式；

a) 檢查網口是否插正確。

b) 對於靜態 IP，要設定正確，否則網路將不通。

c) 對於 DHCP，應確保 DHCP 伺服器工作

（5） 登入時，系統將提示資訊：*“使用者 [username]目前已登入本系統”*。同時，勾選“停止使用者[*username*]”時出錯。

因爲您沒有許可權使該使用者失效。如果仍要登入，請聯繫系統管理員。

（6） 不能訪問 UU100/UU200。

如果您通過 Direct Access 或 Private Access 連接模式不能訪問 UU100/UU200，原因之一可能是 UU100/UU200 或 UUSwitch/UUExchange DNS 名稱解析失敗。請先確認 DNS 名稱解析服務能正確執行。

以下幾種方式會影響 DNS 名稱解析服務。

1. DNS 伺服器指向非預期的地方。
2. DNS 名稱被固化在“hosts”文件中。在 Windows XP/2000 中，該文件被保存在“\windows\system32\drivers\etc”目錄下。
3. IE 代理伺服器設定指向一個已有的 WEB 代理伺服器（無論通過自動檢測還是通過直接分配），該 WEB 代理伺服器可能會將名稱直接指向其他非預期的地方。
4. 啓用了 DNS 客戶端服務，并且可能包含了一個舊的緩存的值。

解決辦法：

請檢測每種可能的情況並確保這些設定均正確。

1. 確認 DNS 伺服器確實爲需要使用的伺服器。
2. 確認您的“hosts”文件沒有被修改，而且設定正確。
3. 確認您的代理伺服器已被正確指定。有時，IE“區域網路設定”代理伺服器一項中的一些核取方塊會無意地被選中。
4. 如果啓用了客戶端服務，電腦中會在緩存中保存以前解析過的主機名稱。該項服務在本系統中作用不大，反而可能會因爲緩存了舊的解析名稱而導致無法正確訪問 UU100/UU200。您可以臨時停用該服務以查看這些問題是否已被解決。

（7） 無法通過 IE 下載客戶端軟體，原因何在，如何解決？

當使用者無法遠端下載客戶端軟體時，請考慮以下兩種可能的原因：

a) 使用者許可權不足；
   該使用者可能不具備下載或安裝 ActiveX 元件的許可權，請聯繫管理員確認。
b) 系統是否不支援 ActiveX 元件的下載；
   和其他大多數 SSL VPN 產品一樣，UU100 用戶端機器對 IE 的安全設定有以下要求：

| **“ActiveX 元件和插件”設定項** | **設定值** |
|---|---|
| 對已標誌爲可安全執行腳本的 ActiveX 元件執行腳本 | 啓用/提示 |
| 下載已簽名的 ActiveX 元件 | 啓用/提示 |
| 運行 ActiveX 元件和插件 | 啓用/提示 |

否則IE將拒絕下載UU100 的客戶端軟體，使用者介面也不會顯示在螢幕上。您可以訪問網頁“http://autos.msn.com/gallery/”（該網頁有一些ActiveX元件）。通過查看是否所有的圖片都能在該網頁正確顯示，由此可驗證是否能排除這種可能。如果這些圖片確實不能在該網頁正確顯示，請修改您機器上的安全設定。

# 第6章 附錄

## 6.1 UUDynamics File Browser Express/ File Browser 使用說明

“UUDynamics File Browser Express”和“UUDynamics File Browser”是 UUDynamics 公司爲客戶提供的兩種遠端檔案訪問服務機制。通過配置 ***i*STAR™**系統架構中 UU100/UU200/UU1000，可以將檔伺服器上的共用檔案安全簡便的發布給遠端的使用者使用。

只需簡單的配置，“UUDynamics File Browser Express”就可以將伺服器端的 Windows Share 顯示在用戶端，通過命令按鈕的使用者介面提供上傳、下載、刪除、更改名稱等操作功能；而“UUDynamics File Browser”則在伺服器端和 IIS/FTP 集成，在用戶端和 Windows Explorer 集成，能提供 Windows 平臺上標準的文件 drag/drop, copy/paste 等完整的文件管理功能，爲了使用此功能，使用者必須瞭解 IIS/FTP 的配置方法。

使用者可以根據不同的情況，選用“UUDynamics File Browser Express”或“UUDynamics File Browser”。

- **UUDynamics File Browser Express**

NetBIOS 目錄共用是基於 NetBIOS 協定，訪問某台伺服器上所有的共用檔案夾；但由于它是基于區域網路的設計，所以在進行跨地域的遠端檔案訪問時，如果從使用者端到遠端伺服器端的網路延遲超過 300-500ms 時，那 NetBIOS 目錄共用就無法工作。UUDynamics File Browser Express 目錄共用在網路的一邊使用 NetBIOS，因此檔伺服器端無需任何修改就能在 UU100/UU200/UU1000 上發佈共用檔案；而在網路的另一邊使用了 HTTP 傳輸機制，使得跨地域傳輸檔案時，既提供易用性又能够避免 NetBIOS 在遠端服務時網路延遲的問題，在廣域網上提供非常好的訪問性能。

UUDynamics File Browser Express 用 Internet Explorer，檔伺服器端無需任何修改就能在 UU100/UU200/UU1000 上發佈共用檔夾。同時，UUDynamics File Browser Express 整合了許可權訪問機制，保護檔案不被未經授權的使用者訪問。目前 UUDynamics File Browser Express 只支援單個的檔案上傳，簡單的檔案管理。

**<u>配置 UUDynamics File Browser Express 服務：</u>**

**1· 配置檔伺服器端：**

發佈 UUDynamics File Browser Express 服務，實際上在檔伺服器端無需額外安裝配置，只需要按照常規共用一個或多個檔夾，爲共用的檔案夾設定合適的訪問許可權。如果需要允許匿名訪問，則需要開啓 Guest 使用者。

對於 Linux 的 File Server，需要將 Linux 機器配置成 SMB Server 或者 NFS Server（只在 UU200 上支援）。

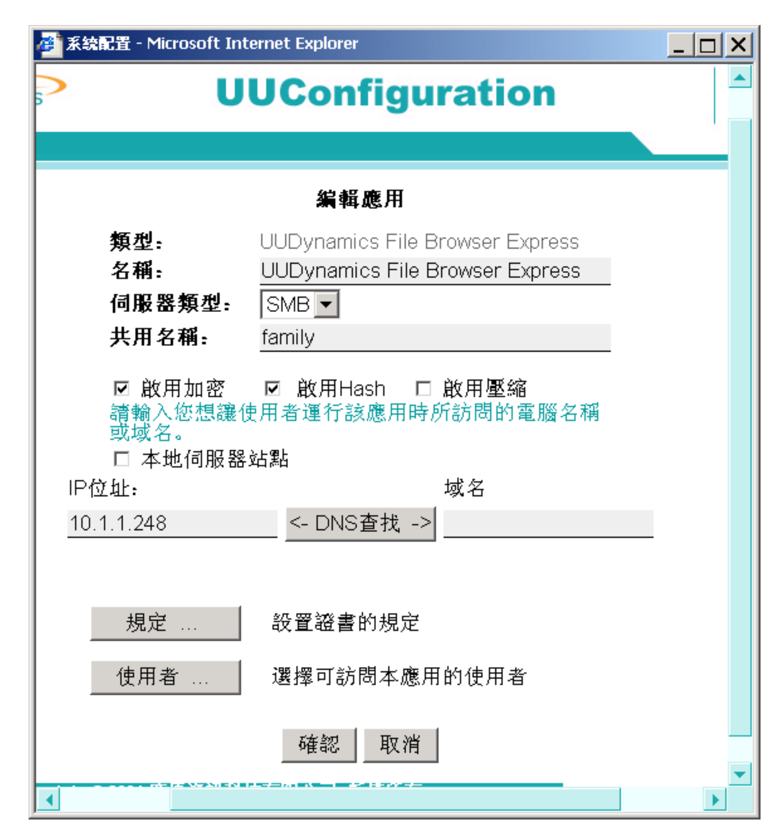
ⓘ 注意：

在發佈 UUDynamics File Browser Express 服務之前，請先驗證共用的檔案夾的設定。您可以通過區域網路訪問某台已共用檔夾的伺服器，驗證是否能够正確訪問這個共用檔夾，訪問許可權設定的是否正確。Windows 2000/XP/2003 的檔伺服器，請檢查域或本地安全策略的設定，以保證授權使用者可以訪問共用檔夾。如果訪問能夠正確執行，就可以正確發佈 UUDynamics File Browser Express 服務。

**2． 配置 UU100/UU200/UU1000：**

在 UU100/UU200/UU1000 上發佈 UUDynamics File Browser Express 服務與發佈其他應用程式類似。發佈應用的詳細方法請參閱“UU100/UU200/UU1000 使用者手冊”中的發佈應用程式（Shared Application Service）部分。

發佈 UUDynamics File Browser Express 服務的介面如附圖 1 所示：




附圖 1

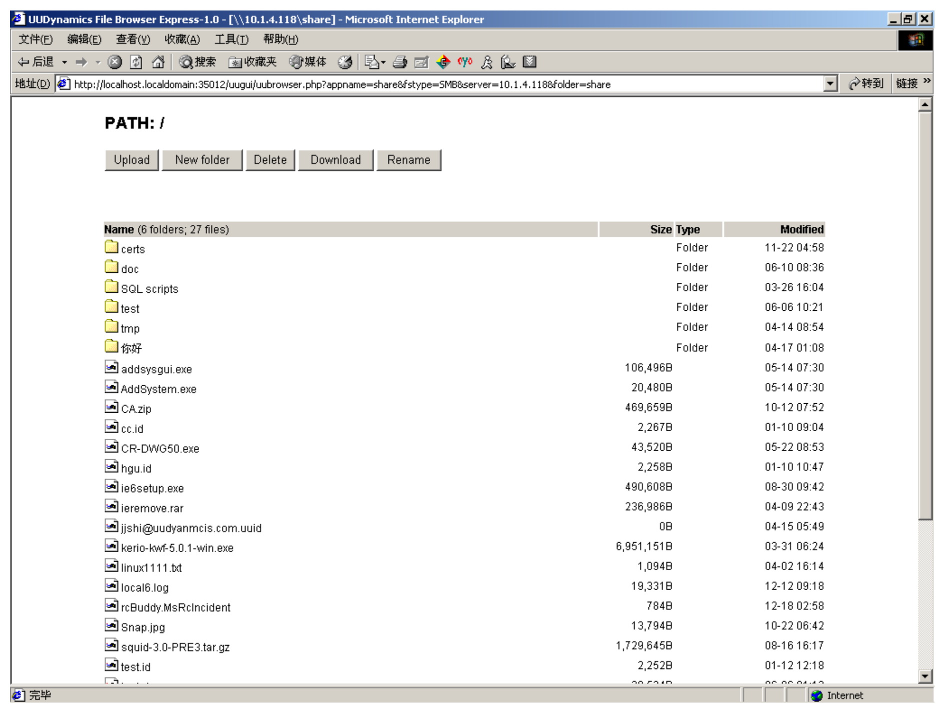
| 參數名稱 | 說明 |
| --- | --- |
| 名稱 | 為這個應用服務取一個名稱，這個名稱將顯示在使用者端的視窗中。如果有多個 UUDynamics File Browser Express 服務，則必須為每一個服務取不同的名稱。 |
| 類型 | 選擇檔伺服器的類型。預設為 SMB，我們在將來會提供更多的可用類型。 |
| 名稱 | 共用檔夾名稱。設定成伺服器上共用名 |

| | 稱，以訪問特定的共用檔夾。[目前不支援中文或其他含特殊字元的共用名稱] |
|---|---|
| 啓用加密/Hash/壓縮 | 選擇加密/Hash 演演算法或壓縮方法。 |
| IP 位址/功能變數名稱 | 檔伺服器的位址或 DNS 名稱。DNS Lookup 的結果依賴於本地 DNS 的配置。 |
| 使用者 | 選擇可以使用這個服務的使用者。 |

例如，一台地址爲 192.168.0.1（DNS 名稱：file.test.uud），共用了名稱爲 share 的檔夾，則共用名稱輸入 “share”，IP Address 輸入 “192.168.0.1” ，或者 DNS 輸入 “file.test.uud” 。

**3． 配置使用者端：**

UUDynamics File Browser Expres 的使用方法與其他被發佈的應用程式的使用方法完全相同。輕按兩下視窗中的 UUDynamics File Browser Expres 的圖表，在新視窗中輸入認證資訊，通過認證就可以進入共用檔夾，使用者可以按照所擁有的許可權，執行標準的檔案操作。File Browser Express 的介面如附圖 2 所示：




附圖 2

其中：

| 按鈕名稱 | 說明 |
|---|---|
| Upload | 表示文檔上傳到遠端文件伺服器上的 Windows share 中 |
| New Folder | 表示在遠端伺服器上的 Windows share 中新建一個子目錄 |
| Delete | 用于刪除一個文件或子目錄 |
| Download | 用于將遠端文件伺服器上的 Windows share 中的文件下載到用戶端 |
| Rename | 用于對文件或子目錄的更改名稱 |

## ● UUDynamics File Browser

Ftp 是常用的一個 C/S（客戶/伺服器）架構的檔案傳輸工具，它在廣域網上有很好的性能。Microsoft IIS 中的 FTP 服務整合 Windows 的認證和訪問控制機制。“UUDynamics File Browser”就是利用 Microsoft IIS 中的 FTP 服務，可以與 Windows 平臺完全整合，在廣域網上提供很好的性能的文檔訪問服務；同時，“UUDynamics File Browser”也可以通過一般的 FTP 伺服器來提供 Linux/UNIX 伺服器上的遠端檔案訪問。由於 UUDynamics File Browser 結合了 IIS 服務，與 UUDynamics File Browser Express 相比提供了完整的檔案操作，使用者可以執行標準的檔案建立、複製、移動和移除等操作；而 UUDynamics File Browser Express 只能做基于按鈕的操作。

**配置 UUDynamics File Browser 服務：**

**1.配置檔伺服器端：**

在 Linux/UNIX 上的配置很簡單，就是一個一般的 FTP 伺服器的配置，這裏不再敍述。以下介紹在 Windows 平臺上配置和使用 UUDynamics File Browser 的方法。

Windows 平臺上的 IIS/FTP 組合不僅提供對本地電腦上的虛擬目錄的存取，還提供通過 FTP 伺服器實現對區域網路上共用資源的存取。有關 IIS/FTP 的配置，本手冊中只做簡單介紹，詳細操作指南請用戶參考 Windows 的相關幫助資訊。

要使用 UUDynamics File Browser 存取遠端檔案，除了部署 iSTAR™產品之外，還要完成以下步驟：

a) 首先要安裝和配置 IIS；

b) 然後在 UU100/UU200/UU1000 上發佈 UUDynamics File Browser 給遠端使用者。

***1.1* IIS 的安裝：**

根據您使用的作業系統不同，你可能需要安裝 IIS。

（1）Microsoft Windows 2000 伺服器/ Microsoft Windows 2000 Advance 伺服器

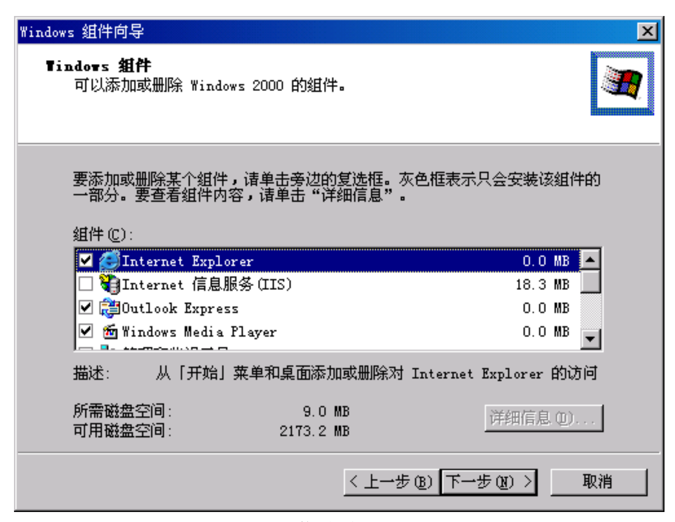
Microsoft Windows 2000 伺服器/ Microsoft Windows 2000 Advance 伺服器上已經預設安裝幷啓動了 Microsoft IIS(如果您的 IIS 沒有啓動，請參考 Microsoft Windows 2000 伺服器/ Microsoft Windows 2000 Advance 伺服器幫助系統，啓動 IIS）

（2）Microsoft Windows 2000 Professional/ Microsoft Windows XP Professional/ Microsoft Windows 伺服器 2003

Microsoft Windows 2000 Professional/ Microsoft Windows XP Professional/ Windows 伺服器 2003 的預設安裝不包括 Microsoft IIS 的安裝，但系統盤包括該軟體，使用者必須手動安裝。

安裝 IIS 的方法如下：

開啓控制面板中的“增加或移除程式”，在“增加或移除程式”視窗中選擇“增加/移除 Windows 組件”後，彈出如附圖 3 所示視窗：




附圖 3

如圖所示，選擇“Internet 資訊服務（IIS）”後,按“下一步”就可以安裝 IIS，您只要根據提示進行操作即可。

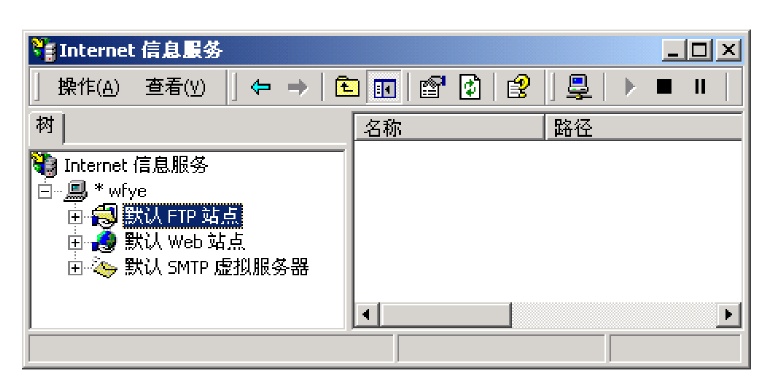
## *1.2* IIS 的配置：

安裝好 IIS 後，您還需配置 IIS 中的 FTP 來指定被遠端存取的 folder 和訪問許可權。

（1）創建 Virtual Directory

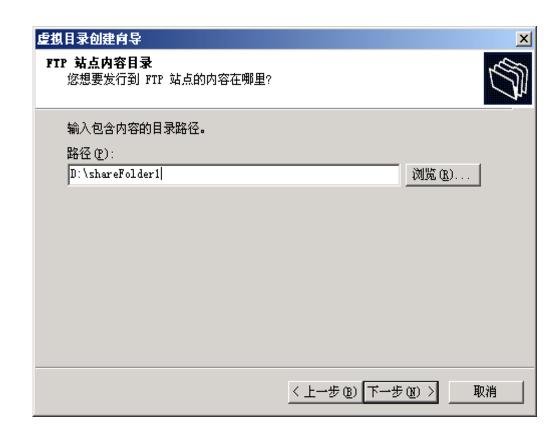
首先確定需要被遠端存取的本地目錄，在 FTP 伺服器上創建虛擬目錄，與該物理目錄連接。具體操作方法如下：

開啓控制面板中的“管理工具”，運行“Internet 服務”管理器（如附圖 4 所示）；配製“預設 FTP 站點”的屬性，選中“預設 FTP 站點”，點選滑鼠右鍵，選擇“新建”->“虛擬目錄”，出現如附圖 5 所示的介面，輸入別名“虛擬目錄名稱”；然後 Browse 或輸入物理錄；如附圖 6，設定該目錄得的訪問許可權；最後按“完成”就創建好了虛擬目錄。

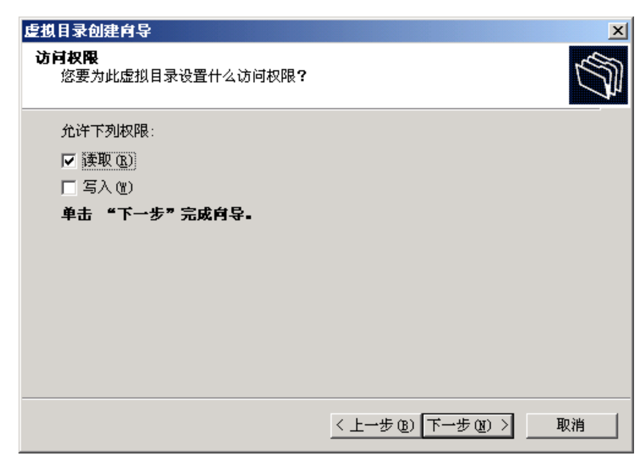



附圖 4



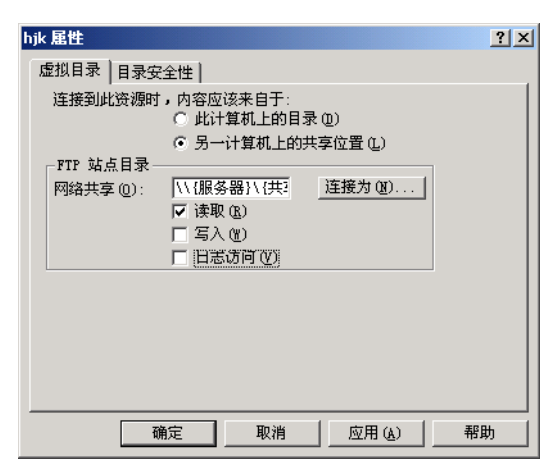

附圖 5




附圖 6

（2）建立連接網路中電腦的共用位置的虛擬目錄

選中某個建好的虛擬目錄，點選滑鼠右鍵，選擇“屬性”，可以看到如附圖 7 所示的視窗：




附圖 7

連接此資源時，內容應該來自於：選擇“另一台電腦上的共用位置”，然後再下面的網路共用中按照“\\伺服器\共用”的格式填入區域網路中的共用位置，再按“連接爲”輸入對此資源訪問的使用者名稱和密碼；最後選擇遠端客戶的訪問許可權。

（3）設定訪問許可權

可以從以下四個方面來設定訪問許可權：FTP 站點許可權設定、NTFS 許可權設定、允許以匿名訪問、啓用 FTP 基本驗證方式。

FTP 站點許可權設定：

IIS 的 FTP 服務器具有靈活的目錄訪問控制，它可限制使用者對站點或目錄的讀、寫許可權，此外它還可根據用戶端 IP 位址進行訪問控制。具體方法如下：開啓 IIS 管理控制臺：開始->程式->管理工具->Internet 服務管理器；右鍵選擇 FTP 站點或虛擬目錄屬性，在主目錄或虛擬目錄屬性頁中，選擇讀取及寫入選項。

NTFS 許可權設定：

FTP 伺服器可以利用 Windows 作業系統中的檔或檔夾的 NTFS 許可權屬性來控制使用者訪問，因此一個使用者若需訪問某個 FTP 站點或目錄，則其必須對該物理目錄有至少讀的許可權。

檔或檔夾的 NTFS 許可權屬性具體的設定方法爲：

開啓 Windows 資源管理器 ，找到 FTP 站點或虛擬目錄所對應的物理目錄，右鍵點選屬性，選擇安全性 ，賦給該 FTP 使用者相應的 NTFS 許可權(讀取，寫入)。

允許以匿名或指定使用者身份訪問：

開啓 IIS 管理控制臺：開始->程式->管理工具->Internet 服務管理器；右鍵選擇 FTP 站點屬性，如附圖 8，選擇安全帳號，勾選“允許匿名連接”。這樣，遠端客戶訪問時就有系統預設使用者 IUSR_…的許可權，您也可以指定一個使用者。



附圖 8

啓用 FTP 驗證：

如果您想讓每一個來訪問的使用者輸入自己的使用者名稱和密碼，擁有自己的許可權，則不要勾選“允許匿名連接” ，這樣就起用了 FTP 基本驗證方式。

對於利用 FTP 基本驗證方式訪問的使用者，其訪問權利除了前面敘述的 FTP 站點許可權和 NTFS 許可權外，還需要使用者許可權設定。

因 FTP 採用基本驗證方式，所以基本驗證的使用者權利要求也適用於 FTP 驗證。基本驗證方式要求訪問的使用者對目標主機具有從網路訪問此電腦和在本地登入兩種許可權。這兩種許可權需要在安全策略中設定。在 Windows2000 中，存在三種安全策略：域

安全策略，本地安全策略，網網網網域控制器安全策略，它們的優先順序為：網網網網域控制器安全策略、域安全策略、本地安全策略。在設定安全策略時需注意有效的策略中允許使用者從網路訪問此電腦和在本地登入兩種許可權。

配置方法為：

如果 FTP 伺服器安裝在網網網網域控制器上，則由于網網網網域控制器安全策略的策略設定優先順序最高，因此我們在網網網網域控制器安全策略中進行策略更改（為減少安全隱患，强烈建議使用者不要在網網網網域控制器上建立 FTP 站點）：

**開始->程式->管理工具->網網網網域控制器安全策略**

如果 FTP 伺服器不是網網網網域控制器(DC)，則由于一般域安全策略中不會對使用者許可權進行設定，因此本地安全策略中的設定也可生效：

**開始->程式->管理工具->本地安全策略**

點選展開本地策略，輕按兩下展開使用者權利指派，在從網路訪問此電腦和在本地登入中檢查該 FTP 使用者是否已具有該許可權，否則，增加該 FTP 使用者。

如果安全策略配置有改動，可用以下命令手動刷新策略配置，使其立即失效：

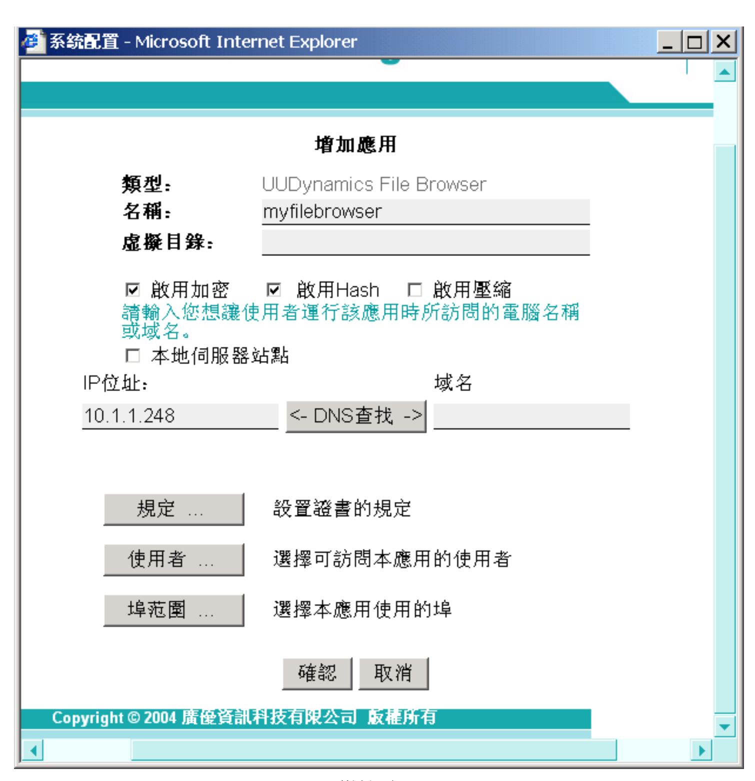
secedit /refreshpolicy machine_policy /enforce

注意：

IIS/FTP 的配置正確與否，可以先在區域網路中進行測試，即在區域網路中選擇一台電腦，啓動 IE,通過 FTP 連接到 FTP 伺服器，執行所需的操作。我們建議只有在區域網路測試成功後，才將它配置到 *i*STAR 上實現遠端操作。

**2．UU100/UU200/UU1000 端配置**

在 UU100/UU200/UU1000 上發佈 UUDynamics File Browser 的方法請參見“UU100/UU200/UU1000 使用手冊”中的發佈應用程式（Shared Application Service）部分。 發佈“UUDynamics File Browser”的介面如附圖 9 所示，除了和其他應用一樣需要填寫共用應用名稱及所在伺服器位址或名稱外，還需填寫 Virtual Directory 名稱，即 IIS 伺服器端設定的別名。




附圖 9

其他有關設定請參見本手冊第 4 章。

**3．配置使用者端：**

UUDynamics File Browser 在使用者端的使用和其他被發布的應用程式沒有任何區別，輕按兩下視窗中 UUDynamics File Browser 的圖示（即 IE 的圖示），我們的軟體會自動將 FTP 設定成 Passive 模式，使用者可以執行標準的檔案建立、複製、移動和移除等操作。

## 6.2 iSTAR™支援的客戶/伺服器應用

市場上不同的 SSL VPN 產品所支援的應用屬於以下幾種情況：

1． 基於 Web 的應用的逆向代理：

這種方法僅僅支援那些被 Web 化的應用，就是用 Web 工具開發且客戶端是 Internet 瀏覽器的應用。

2． 傳統應用的客戶/伺服器工具：

由於大量應用是在 Web 時代前開發的，這種類型已經變成任何 SSL VPN 的必備功能。大多數廠商用 ALG(應用層閘道)來支援這類應用，即爲一些流行的應用（如 Outlook, Lotus Notes, Telnet 等）提供專門的或特定的支援。這種方法需要在用戶端安裝專門的客戶端軟體。

3． 遠端虛擬接入：

這一種全能的方法，它可以解決前面兩種方法解決不了的問題。所有的廠商都採用傳統的 VA(虛擬網卡)機制來將一個本地電腦虛擬接入遠端網路。由于這種機制建立在第三層網路結構上的，用戶端和伺服器端必須解決好可能的 IP 位址不相容的問題。

在不同 Microsoft 平臺上的 ***iSTAR***™用戶端是 ***iSTAR***™體系結構中最重要的元件之一，***iSTAR***™支援所有三類應用，但和我們的競爭者不同的是，***iSTAR***™用一個通用的工具來支援客戶/伺服器軟體，包括幾乎所有的傳統客戶/伺服器應用軟體。儘管爲了確認對客戶應用的

支援，***i*STAR™**還是需要“應用認證”，但提交到我們驗證中心的應用軟體中還沒有不被***i*STAR™**支援的。借助于這個强大的用戶端軟體工具，***i*STAR™**在一個統一、通用的框架下支援上述的 1，2 項，基于這個統一的框架，伺服器的管理也被大大簡化了。

本文檔試圖要定義由 ***i*STAR™**的通用客戶工具支援的這類客戶/伺服器應用。下列的條件只適用于第 1 和 2 類。

### 6.2.1 用戶端到伺服器端

***i*STAR™**是通過“虛擬化”用戶端應用來實現對客戶/伺服器應用的支援的。所有的網路環境和操作被 ***i*STAR™**的客戶軟體截獲並隨即被 ***i*STAR™**發布單元代理傳輸到伺服器端。這種虛擬化的運行對於特定啓動的應用是透明的。

注意，只有用戶端的網路操作被代理了，TCP/IP 的操作必須從用戶端發起；伺服器邏輯獨立於 ***i*STAR™**而運行，所以不允許發起對用戶端的網路操作。

### 6.2.2 對網路資料包中的用戶端位址的敏感性

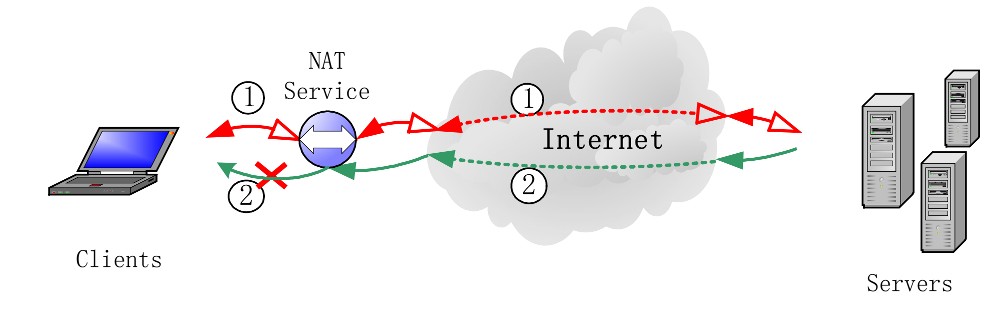
由於 ***i*STAR™**虛擬化用戶端應用，所以那些發出包含用戶端的網路環境裏的 IP 位址的網路包的應用不能被支援。

### 6.2.3 支援 IP 應用及特定的 NetBIOS 應用

***i*STAR™**客戶軟體僅支援 TCP/IP 應用。原始的 NetBIOS 不能支援，但有一類 NetBIOS 除外，即由 UUDynamics 提供了的“**Custom – Network drive based C/S**”應用（詳細內容請參考“4.2 定制新的應用程式” 中的例二）。

### 6.2.4 NAT(網路位址轉換)的友好性

伺服器不能發起對用戶端網路操作，而且網路資料包不能包含用戶端的 IP 位址資訊，有一個簡單的測試可以來判斷應用是否滿足這個規定。應用必須能從 NAT 後面運行，去訪問 NAT 外的伺服器。換句話說，滿足條件的應用必須是 NAT 友好的。




附圖 10

**Passive 應用：**

如果是這種應用，由 Client 端發起的 TCP 連接請求經過 NAT 伺服器到達伺服器端（如

連接①→所示），伺服器端僅利用原有連接將資料包返回 Client 端（如連接①←所示）。這種應用由於使用的是已有的連接通道，因而可以真正送達 Client 端。

這種應用的典型例子有 Data 模式的 Netmeeting 應用及 FTP 服務等。

***i*STAR™**支援這類應用。

**Active 應用：**

如果是這種應用，由 Client 端發起的 TCP 連接請求經由連接穿越 NAT 伺服器到達伺服器端（如連接①→所示），伺服器端會將許多其他控制資訊（如 IP 位址、埠等）連同資料包一起打包，沿著新建的連接（連接②）返回 Client 端。由於這種資料包無法穿透 NAT 伺服器，因而不能真正送達 Client 端。這種應用的典型例子有語音模式的 Netmeeting 應用。

對於這類應用，***i*STAR™**暫不支援。

## 6.2.5 WinSock 應用

支援的應用必須基於 Windows WinSock。

# 術語表



# 10~15 劃

## 第三方證書（數位元電子憑證）

第三方證書是用於該 UU200 和使用者端之間建立 https 安全連接時所需的標識該伺服器的數位證書。

從第三方發證機構處獲得數位元憑證的申請的方式及費用可以參考以下兩個網站。

http://www.hitrust.com.tw/hitrustexe/frontend/verisign_price.asp

http://www.globaltrust.com.tw/apply/index.html

某些發證機構所簽發的數位憑證，其根憑證沒有被 Microsoft 公司預先包括在其 IE 的受信任根憑證資料庫之中，在這種情況下，除非使用者將該根憑證輸入到使用者的 IE 瀏覽器根憑證資料庫中，不然會在使用者端跳出一個警告資訊，此時使用者可以用<查看證書>功能鍵檢視數位憑證的詳細內容，待確定之後，按<是>鍵繼續進行操作。

無論第三方發證機構的根憑證有沒有被 Microsoft 公司預先包括在其 IE 的受信任根憑證資料庫之中，都不會影響 iSTAR™的功能。

以下這個網站有詳述User如何製作自身的CSR檔案，然後再至認證中心申請憑證檔。

http://www.globaltrust.com.tw/support/index.html

http://www.openssl.org/related/binaries.html

**注意事項：**

- 申請的憑證必須符合 Apache Server 的格式。客戶或經銷商可以利用 OpenSSL 產生 CSR 檔案。
- 由於涉及資訊安全，建議客戶自行辦理較好。
- 建議經銷商或客戶在申請電子憑證時，最好是選擇 DNS Name 而不是 IP。
- 通常辦理電子憑證需，在資料齊全的情況下，應該一個工作天可以完成。

## 連接方式

UU200 有兩種接入方式供使用者選擇：Direct Access 和 Private Access。

- Direct Access

  如果希望遠端使用者通過 Public IP 訂閱由 UU200 發佈的應用，可選擇該連接方式。

  該方式下, UU200 需要預先準備公共靜態 IP 位址以及閘道、子網掩碼和 DNS。

  此外，爲了使用者端能與它建立 SSL 連接，UU200 上還需要一張數位元元電子憑證。您可以申領一張第三方（如 VeriSign 或 Globaltrust 等）的證書，也可以直接使用系統預設的 UUDynamics 公司的證書。

  **說明：**

  有關第三方證書的獲取和注意事項，請參閱“術語表”之“第三方證書”。

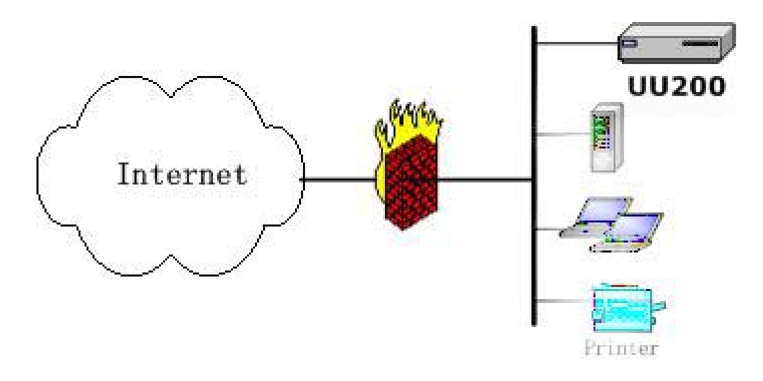
- Private Access

  如果希望遠端使用者通過 Private IP 訂閱由 UU200 發佈的應用，可選擇該連接方式。

  當 UU200 通過 UUSwitch 或 UUExchange 連接時，需要爲 UU200 準備 UUID、私有 IP 位址以及閘道、子網掩碼和 DNS。

# 網路模式

UU200 在網路中有三種模式可供選擇：單模式、透明模式和路由模式。您可以根據您的網路結構參考下面的說明來選擇一種模式。



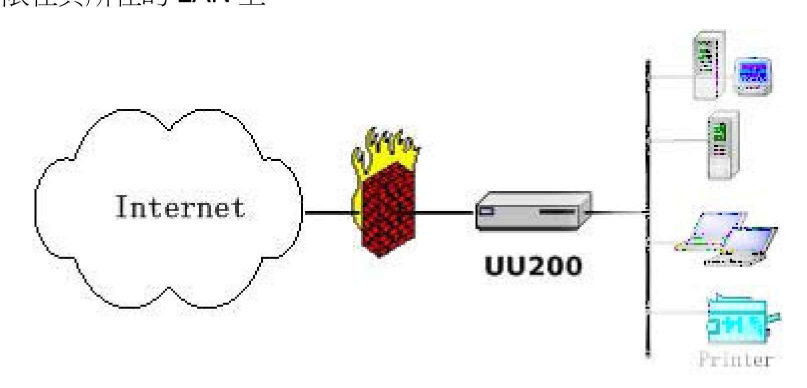

單模式示意圖

**單模式**：是 UU200 被放置于內部網路中的任意位置的一種模式（見上圖）。

連接方式：UU200 的第 4 網口與您的內部網路相連接。

特點：不改變原網路中的任何設備狀態，配置簡便、快捷。需要時，插到連接網際網路的內部網路上就可使用。可以使其所在的 LAN 得到安全的網路保護。

如果需要發佈整個子網（即 LAN to LAN，參見本手冊“4.2 發布子網”部分）時需要在原有路由器或使用者端增加路由。網路安全保護只限在其所在的 LAN 上。

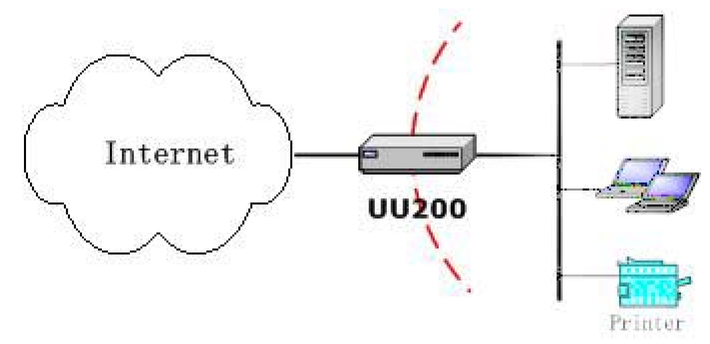



透明模式示意圖

**透明模式**：是 UU200 被放置于內部網路和防火墻或路由器之間的位置的一種模式。

連接方式：UU200 的第 **1** 網口與內部網路相連，UU200 的第 **4** 網口與防火牆或路由器相連。

特點：配置時不需要變更原有路由器或使用者端的任何配置。可以使在其後面的整個網路得到安全的保護。




路由模式示意圖

**路由模式**：是 UU200 被放置于防火墻或路由器的位置的一種模式，即 UU200 取代了防火墻或路由器。
連接方式：UU200 的第 **1** 網口與內部網路相連，UU200 的第 **4** 網口與外部網路相連。
特點：在提供 Publisher 功能的同時，也提供了防火墻或路由器功能。

**說明：**
配置時爲了減少影響網路的日常運行，建議先連接到某個 LAN 上進行配置，然後再移到指定的模式位置上。

# A~Z

## DMZ/DDMZ

（非軍事區）是放置公共資訊的最佳位置，您可以將一些必須公開的伺服器設施，如企業 Web 伺服器、FTP 伺服器和郵件伺服器等這樣的服務放置在這個區域中，而將公司中的機密的和私人的資訊可以安全地存放在內網中，即 DMZ 的後面。這樣使用者、潛在使用者和外部存取者都可以直接獲得他們所需的關於公司的一些資訊，而不用通過內網。

UU200 爲您提供了一種設定和管理 DMZ 的服務——動態 DMZ（即 DDMZ：Dynamics DMZ）。所謂 DDMZ，是指您可以根據您現在的網路狀況，靈活的選擇 UU200 所處的位置，您可以將 UU200 配置爲網路中的第一台防火墻，或是將它放在已有防火墻之後，以得到增强的安全性。

UU200 的 DDMZ 通過這一系列安全策略的組合，幫助您將一些在已在 DMZ 中配置好的服務，例如檔伺服器，WEB 伺服器，FTP 伺服器等，發佈給外部存取者和需要這些公共服務的使用者，而不用擔心對公司內部網路的未授權的存取。

## UUID

UUID 由主模式 UUSwitch（/UUExchange）分配。UUID 必須是唯一的。用于有效標識發布單元 Publisher（例如：UU100,UU200），以及子模式 UUSwitch(/UUExchange)。
如果 Publisher 的連接方式爲 Private Access 方式，則該 Publisher 必須擁有一個唯一的 UUID。在啓動時 Publisher 用 UUID 註冊到 UUSwitch（/UUExchange）,從而成爲整個 ***i*STAR™**的一部分。
UUID 的格式如 Email 一樣：AAA@bbb.ccc，其中 bbb.ccc 是 Domain 名，例如：aaa@uudynamics.com。
在安裝 Publisher 前，請先聯繫 UUSwitch（/UUExchange）管理員獲取壓縮的 UUID 檔案。